



**Считыватель Sigur MR100.  
Описание и инструкция  
по эксплуатации**

**Редакция от 02.06.2023.**

## Оглавление

1.	Введение .....	4
2.	Технические характеристики .....	5
3.	Комплект поставки .....	7
4.	Общие функции считывателя в СКУД Sigur .....	8
5.	Монтаж считывателя .....	9
5.1.	Назначение проводов считывателя .....	9
5.2.	Общие рекомендации к монтажу считывателя .....	10
5.3.	Рекомендации по выбору кабелей .....	10
6.	Индикация считывателя .....	12
6.1.	Сигналы управления индикацией .....	12
6.1.1.	Управление индикацией при подключении по Wiegand .....	12
6.1.2.	Управление индикацией при подключении по OSDP .....	13
6.1.3.	Стандартные профили индикации считывателя .....	15
6.2.	Настройка пользовательской индикации считывателя .....	16
6.2.1.	Создание профиля индикации считывателя .....	17
6.2.2.	Создание реакции считывателя .....	22
6.2.3.	Добавление звука реакции считывателя .....	24
6.2.4.	Способы загрузки пользовательского профиля индикации на считыватель .....	25
7.	Настройка реакции на вскрытие корпуса считывателя .....	28
8.	Программирование считывателей .....	30
8.1.	Программирование считывателя мастер-картой .....	31
8.2.	Программирование считывателя конфигурационным файлом .....	32
8.3.	Программирование считывателя через протокол SSDP .....	34
9.	Сброс параметров считывателя к заводским настройкам .....	36
9.1.	Аппаратный сброс .....	36
9.2.	Сброс параметров считывателя через приложение «Настройки» .....	36
9.3.	Параметры работы считывателя по умолчанию .....	37
10.	Настройка доступа ПО Sigur к почтовым серверам .....	38
10.1.	Настройка параметров сервера исходящей почты .....	38
10.2.	Настройка параметров сервера входящей почты .....	38
11.	Работа с картами Mifare .....	40
11.1.	Работа в незащищённом режиме, чтение UID .....	40
11.2.	Работа в защищённом режиме .....	40
11.2.1.	Настройка работы с картами Mifare Classic 1K/4K .....	40
11.2.2.	Настройка работы с картами Mifare Plus .....	41
11.2.3.	Правила заполнения служебных полей настроек карт Mifare .....	42
12.	Работа с банковскими картами .....	44
12.1.	Чтение UID или эмуляция Mifare банковской картой .....	44
12.2.	Чтение PAN-номера банковской карты .....	45
13.	Чтение карт EM Marine и HID® ProxCard II .....	46
14.	Занесение карт в ПО Sigur .....	47
15.	Работа со смартфонами в качестве идентификатора .....	48
15.1.	Идентификация по смартфону, общие сведения .....	48
15.2.	Настройка системы на работу со смартфонами .....	48

15.3.	Добавление мобильных идентификаторов в ПО .....	51
15.3.1.	Отправка пригласительного письма .....	52
15.3.2.	Групповая отправка пригласительных писем .....	53
15.3.3.	Отправка ответного письма .....	53
15.4.	Работа с приложением «Доступ» .....	55
16.	Приложение «Sigur Настройки» .....	58
16.1.	Назначение приложения «Sigur Настройки» .....	58
16.2.	Поиск считывателей в радиусе действия BLE смартфона .....	58
16.3.	Обновление внутреннего ПО считывателя .....	60
16.4.	Установка специального внутреннего ПО считывателя .....	62
16.5.	Загрузка профиля конфигурации чтения на считыватель .....	64
16.6.	Сброс конфигурации чтения считывателя .....	68
16.7.	Загрузка профиля индикации на считыватель .....	68
16.8.	Сброс конфигурации индикации считывателя .....	73
16.9.	Настройка выходного интерфейса считывателя .....	73
17.	Шифрование данных, передаваемых по OSDP .....	75
17.1.	Создание профиля шифрования OSDP .....	75
17.2.	Применение профиля шифрования OSDP .....	76
17.3.	Сброс профиля шифрования .....	80
17.4.	Изменение профиля шифрования .....	82
18.	Обновление внутреннего ПО считывателя через программу «Клиент» .....	84
19.	Журнал системных событий .....	86
20.	Общие требования к смартфонам и ПО .....	90
21.	Логика обработки идентификаторов .....	92
21.1.	Чтение карты .....	92
21.2.	Чтение смартфона .....	93
22.	Контакты .....	95

# 1. Введение

Данный документ содержит описание и инструкцию по эксплуатации считывателя Sigur MR100.

Считыватель представлен в трёх модификациях: MR100 Lite, MR100, MR100 Multi.

Считыватели Sigur MR100 предназначены для использования в составе систем контроля доступа и позволяют использовать различный набор идентификаторов в зависимости от модификации.

Все модификации считывателя MR100 (MR100 Lite, MR100, MR100 Multi) позволяют использовать идентификаторы стандарта Mifare (Ultralight, Classic, Mini, ID, DESFire, Plus), в том числе, защищенный режим для семейства Mifare Classic, защищенные режимы SL1 и SL3 для семейства Mifare Plus, а также банковские бесконтактные карты МИР, Visa и MasterCard. Для использования банковской карты в качестве идентификатора должно быть выполнено одно из следующих условий:

1. Поддержка технологии EMV.
2. Наличие статического UID (для использования карты в режиме чтения UID).
3. Наличие эмуляции карт Mifare Classic или Plus, соответствующей документу "AN10833 MIFARE Type Identification" компании NXP (для работы с картами в защищенном режиме).

Модификации считывателя Sigur MR100 и MR100 Multi дополнительно позволяют:

- Проходить идентификацию по смартфону, используя технологию BLE (Bluetooth Low Energy) и/или HCE (Host-based Card Emulation). Поддерживаются смартфоны с ОС Android (BLE, HCE) и iOS (BLE).
- Проходить идентификацию по PAN-номеру банковской карты.

Модификация MR100 Multi в дополнение к вышеуказанному позволяет также использовать карты стандартов Em-Marine и HID ProxCard II (125kHz) в качестве идентификатора.

## 2. Технические характеристики

### Технические характеристики.

Модификация считывателя:	MR100 Lite	MR100	MR100 Multi
<b>Формат поддерживаемых идентификаторов</b>	<ul style="list-style-type: none"> <li>Mifare (Ultralight, Classic, Mini, ID, DESFire, Plus), включая защищенные режимы SL1 и SL3 семейства Mifare Plus, защищенный режим семейства Mifare Classic.</li> <li>Бесконтактные банковские карты MasterCard, Visa, МИР в режиме чтения UID при наличии статического UID/в защищенном режиме при наличии эмуляции Mifare Classic или Plus, соответствующей документу "AN10833 MIFARE Type Identification" компании NXP.</li> <li>Все идентификаторы стандарта ISO14443-A в режиме чтения UID.</li> </ul>		
		<ul style="list-style-type: none"> <li>Смартфоны Android по технологиям NFC и BLE.</li> <li>Смартфоны iOS по технологии BLE.</li> <li>PAN-номер банковской карты по технологии EMV (MasterCard, Visa, МИР, в т.ч. добавленные в электронные кошельки: МИР Pay, Google Pay, Apple Wallet, Samsung Pay).</li> </ul>	
			<ul style="list-style-type: none"> <li>Em-Marine</li> <li>HID ProxCard II (125 kHz)</li> </ul>
<b>Технические параметры</b>			
Дальность чтения карт	До 9 см (в зависимости от карты, режима работы и места установки).		
Дальность чтения смартфонов	-	До 10 метров при прямой видимости (в зависимости от модели смартфона, режима работы и места установки).	
Интерфейс для связи с контроллером	Wiegand настраиваемой битности (26, 34, 58) OSDP (RS485)		
Габариты	90x90x12 мм		
Вес	Вес брутто – 285 г; Вес нетто – 170 г		
Температурный режим	от -40 до +60 °C		

<b>Модификация считывателя:</b>	<b>MR100 Lite</b>	<b>MR100</b>	<b>MR100 Multi</b>
Класс защиты	IP65		
Напряжение питания	12 В (9...28 В)		
Потребляемый ток	90 мА в режиме ожидания, 130 мА при чтении идентификатора.		
<b>Индикация</b>			
Световая	Многоцветный светодиодный индикатор.		
Звуковая	Широкополосный акустический динамик, РСМ 16 бит 44.1 кГц моно.		
Поддерживаемые звуковые форматы	.wav, .aiff, .au		
Длительность загружаемых звуков	Не более 45 секунд.		
<b>Средства диагностики</b>	Датчик открытия корпуса. Датчик температуры. Оцифровка напряжения питания.		

### 3. Комплект поставки

Комплект поставки.

Номер	Позиция	Количество
1	Считыватель Sigur MR100	1 шт.
2	Настенная панель	1 шт.
3	Ключ	1 шт.
4	Комплект крепежа	1 шт.
5	Набор соединителей ScotchLock	1 шт.
6	Инструкция по монтажу	1 шт.

## 4. Общие функции считывателя в СКУД Sigur

Считыватель Sigur MR100 (Lite, Multi) совместим со СКУД Sigur, а также с большинством других систем контроля доступа.

Считыватель поддерживает работу со следующими типами идентификаторов (конкретный набор зависит от используемой модификации считывателя):

- картами формата Mifare Classic (в том числе Mini и ID), Ultralight, DESFire, Plus в режиме чтения их уникального идентификатора – UID. Поддерживается защищённый режим работы Mifare Classic 1K/4K, а также режим SL3 карт Mifare Plus;
- любыми другими идентификаторами стандарта ISO 14443-A в режиме чтения UID;
- бесконтактными банковскими картами МИР, Visa и MasterCard в режиме эмуляции карт Mifare;
- бесконтактными банковскими картами в режиме чтения PAN-номера карты;
- смартфонами с ОС Android или iOS по технологии BLE (Bluetooth Low Energy) при установленном мобильном приложении «Доступ»;
- смартфонами с ОС Android по технологии HCE (Host Card Emulation) при установленном мобильном приложении «Доступ»;
- картами формата EM Marine;
- картами формата HID ProxCard II (125 kHz).

Считыватель оснащён:

- OSDP–выходом;  
Считыватель MR100 (MR100, MR100Lite, MR100Multi) можно подключить по OSDP к контроллерам любых производителей, поддерживающие стандарт OSDP версии 2.2.  
Если считыватель подключается по интерфейсу OSDP к контроллеру Sigur (E2, E4), то взаимодействие происходит по протоколу SSDP (Sigur Supervised Device Protocol), который имеет расширенный функционал характерный только для оборудования Sigur.
- Wiegand–выходом настраиваемой битности;
- многоцветным световым индикатором;
- широкополосным акустическим динамиком;
- тремя цифровыми входами для управления индикацией считывателя (активны при работе контроллера со считывателем по Wiegand);
- средствами самодиагностики, в том числе датчиком вскрытия корпуса, датчиком температуры и датчиком замера питающего напряжения.



## 5. Монтаж считывателя

Процедура монтажа считывателя подробно описана в прилагаемом к считывателю руководстве по монтажу. Актуальную версию документа так же можно найти на [странице](#).

### 5.1. Назначение проводов считывателя



Для подключения считывателя к контроллеру СКУД обратитесь к документации контроллера данной СКУД.

Ниже представлена таблица, описывающая назначение проводов считывателя Sigur MR100.

#### Назначение проводов считывателя Sigur MR100.

Цвет	Название	Назначение
Красный	+12 V	«Плюс» напряжения питания
Чёрный	GND	«Общий» напряжения питания, линий данных и управления
Зелёный	Data 0	Линия данных Wiegand 0 или A (RS-485)
Белый	Data 1	Линия данных Wiegand 1 или B (RS-485)
Синий	IN1/GREEN	Первый цифровой вход управления индикацией считывателя.  Если считыватель находится в заводской конфигурации, то при активации входа следует включение звукового и светового сигнала разрешения доступа.
Коричневый	IN2/RED	Второй цифровой вход управления индикацией считывателя.  Если считыватель находится в заводской конфигурации, то при активации данного следует включение звукового и светового сигнала запрета доступа.

Цвет	Название	Назначение
Жёлтый	IN3/SOUND	<p>Третий цифровой вход управления индикацией считывателя.</p> <p>Если считыватель находится в заводской конфигурации, то при активации входа следует включение звукового и светового сигнала ожидания дополнительного действия.</p> <p>Вход используется также для аппаратного сброса считывателя к заводским настройкам.</p>

## 5.2. Общие рекомендации к монтажу считывателя

Располагать считыватели лучше всего на некотором расстоянии друг от друга, чтобы один и тот же идентификатор не попадал в зону действия сразу нескольких считывателей:

- для карт расстояние между считывателями должно быть не меньше 15 см;
- для смартфонов расстояние определяется настроенным уровнем сигнала.

Не рекомендуется устанавливать считыватель:

- на металлических плоскостях, вблизи источников радиопомех и силовых линий - это снижает дальность чтения идентификаторов, в том числе дальность чтения мобильных телефонов.
- в местах, подвергающихся длительному воздействию прямых солнечных лучей - это повышает вероятность перегрева устройства, сопровождающееся отключением звукового динамика.

## 5.3. Рекомендации по выбору кабелей

При подключении так же ознакомьтесь с рекомендациями от производителя контроллера, к которому будет выполняться подключение.

### Подключение по Wiegand

На небольшом удалении считывателей от контроллера (до 50м) рекомендуется выполнять кабелем сечением 0,22-0,5 мм<sup>2</sup>.

Допустимо использование любых типов сигнальных кабелей, например, КСПВ 8x0,5.

При большей удалённости (50-100 м) необходим кабель большего сечения (0,75-1,0 мм<sup>2</sup>), как минимум, на линиях питания считывателей.

#### **Подключение по OSDP**

Рекомендуется выполнять кабелем типа UTP 5 категории, либо специальными кабелями (например, для внутренней проводки - КИПЭВ, КИПвЭВ, для наружной – КИПЭП, КИПвЭП).

Допускается использование свободных линий связи, проложенных на объекте, выполненных кабелем не ниже третьей категории (ЛВС, телефония). Не допускается прокладка линии связи рядом с силовыми кабелями переменного тока и кабелями управления мощными устройствами.

Электрические характеристики интерфейса RS485 позволяют при соблюдении правил монтажа создавать сегменты линии связи до 1200 метров.

## 6. Индикация считывателя

### 6.1. Сигналы управления индикацией

Независимо от конфигурации индикации считыватель воспроизводит особые звуковые сигналы при включении, аппаратном сбросе и при программировании мастер-картой. Также при установлении связи со считывателем и обменом данными через приложение «Настройки» или «Доступ» загорается оранжевый светодиод. Логика управления индикацией отличается для случаев, когда на считывателе загружена стандартная индикация и когда загружена пользовательская конфигурация индикации.

#### 6.1.1. Управление индикацией при подключении по Wiegand

При подключении по протоколу Wiegand считыватель Sigur ожидает управление индикацией по какому-либо из трех его цифровых входов «IN1/GREEN», «IN2/RED» или «IN3/SOUND».

Активный уровень линий управления – ноль вольт.

##### Подключение по Wiegand, стандартная конфигурация индикации

- Если ни на один из управляющих входов «IN1/GREEN», «IN2/RED» или «IN3/BEEP» не было подано сигнала, то при чтении любого идентификатора считыватель реагирует звуковым сигналом «Разрешение доступа» и кратковременно моргает зеленым.
- Если на одну из управляющих линий «IN1/GREEN» или «IN2/RED» подаётся сигнал, то считыватель переводится в режим внешнего управления индикацией. Считыватель перестаёт сопровождать индикацией чтение любого идентификатора, ожидая управление по какой-либо из линий «IN1/GREEN» или «IN2/RED».

В случае подачи сигнала на линию «IN1/GREEN» один раз воспроизводится звук «Разрешение доступа» и светодиод светится зелёным на время, совпадающее с временем действия управляющего сигнала.

В случае подачи сигнала на линию «IN2/RED» один раз воспроизводится звук «Запрет доступа» и светодиод светится красным на время, совпадающее с временем действия управляющего сигнала.

- Если на управляющую линию «IN3/SOUND» подаётся сигнал, то периодически воспроизводится звуковой сигнал «Ожидание действия» и светодиод мигает оранжевым (0,2 с - оранжевый, 0,2 с - отсутствие цвета). Продолжительность воспроизведения звукосветовой последовательности совпадает со временем управляющего сигнала.

### **Подключение по Wiegand, пользовательская конфигурация индикации.**

Если на считыватель загружена пользовательская конфигурация индикации, то от считывателя может последовать соответствующая, заранее установленная реакция (если на текущий момент нет более приоритетной реакции):

- К считывателю был поднесен и успешно прочитан идентификатор – воспроизводится реакция, установленная на событие «Прочитан идентификатор».
- Считыватель закреплён на настенной панели – воспроизводится реакция, установленная на событие «Считыватель на стене».
- Считыватель извлечен из настенной панели – воспроизводится реакция, установленная на событие «Считыватель оторван».
- Если температура считывателя вышла за пределы нормы – воспроизводится реакция, установленная на событие «Температура вне нормы».
- Если линия «IN1/GREEN» замкнута на GND (не замкнута на GND) – воспроизводится реакция, установленная на событие IN1/GREEN активно (IN1/GREEN не активно).
- Если линия «IN2/RED» замкнута на GND (не замкнута на GND) – воспроизводится реакция, установленная на событие IN2/RED активно (IN2/RED не активно).
- Если линия «IN3/Beep» замкнута на GND (не замкнута на GND) – воспроизводится реакция, установленная на событие IN3/Beep активно (IN3/Beep не активно).

### **6.1.2. Управление индикацией при подключении по OSDP**

При подключении считывателя по протоколу OSDP команды управления индикацией передаются на считыватель Sigur по линиям «А» и «В». Также индикацией можно управлять и по отдельным линиям «IN1/GREEN», «IN2/RED» и «IN3/SOUND».

При подключении считывателя к контроллеру Sigur по OSDP контроллер переходит в режим управления индикацией считывателя на этом порту по линиям "А" и "В". Тем не менее считыватель MR100 в данном режиме продолжает обрабатывать состояние входов IN1, IN2, IN3 и реагировать на изменение состояния соответствующей индикацией. Поэтому опционально для контроллера Sigur можно настроить управление индикацией считывателя по этим линиям.

Конфигурация управления индикацией может быть изменена пользователем.

#### **Управление индикацией по OSDP/SSDP, стандартная конфигурация индикации.**

Если на считыватель не загружена пользовательская конфигурация

индикации, то при чтении любого идентификатора считыватель реагирует звуковым сигналом и кратковременно моргает зеленым.

### **Управление индикацией по OSDP/SSDP, пользовательская конфигурация индикации.**

Если на считыватель была загружена конфигурация индикации, то от считывателя может последовать соответствующая, заранее установленная реакция на определенные события (если на текущий момент нет более приоритетной реакции).

Так как при подключении считывателя по OSDP происходит двунаправленное взаимодействие между считывателем и контроллером, соответственно, события, на которые может отреагировать считыватель, делятся на два типа: события, генерируемые самим считывателем, и события, генерируемые контроллером.

События, генерируемые считывателем MR100:

- «IN1/GREEN активно» («IN1/GREEN не активно») - линия «IN1/GREEN» замкнута на GND (не замкнута на GND);
- «IN2/RED активно» («IN2/RED не активно») - линия «IN2/RED» замкнута на GND (не замкнута на GND);
- «IN3/Beep активно» («IN3/Beep не активно») - линия «IN3/Beep» замкнута на GND (не замкнута на GND);
- «Считыватель на стене» - считыватель закреплён на настенной панели;
- «Считыватель оторван» - считыватель извлечён из настенной панели;
- «Прочитан идентификатор» - к считывателю был поднесён и успешно прочитан идентификатор;
- «Температура вне нормы» - температура считывателя вышла за пределы нормы;
- «Напряжение питания вне нормы» – напряжение считывателя вышло за пределы нормы.

События, генерируемые контроллером Sigur:

- «Ожидание прохода» - объекту доступа был разрешён доступ, контроллер ожидает, когда объект доступа совершит проход;
- «Взлом» - был зафиксировано пересечение точки доступа несанкционированным образом;
- «Удержание двери» - датчик открытия двери не возвращён в нормальное состояние до истечения времени, установленного в настройках точки доступа параметром «Время до сигнала «Удержание двери»».
- «Тревога охранного шлейфа» - от охранного шлейфа контроллера Sigur (E2, E4) поступило событие «Тревога». Считыватель будет реагировать на приходящее событие «Тревога» только от того шлейфа, который назначен точке доступа, к которой непосредственно относится считыватель.
- «Ожидание санкции оператора» - для идентифицированного объекта

- доступа применяется режим с установленной опцией «Требовать санкции оператора на проход», идёт ожидание решения оператора.
- «Ожидание PIN-кода» - для идентифицированного объекта доступа применяется режим с установленной опцией «Дополнительно запрашивать PIN код», контроллер ожидает получения кода от подключенной кодонаборной панели.
  - «Ожидание второй карты» - для идентифицированного объекта доступа применяется режим с установленной опцией «Доступ в сопровождении» или «Доступ только вдвоём», идёт ожидание идентификации сопровождающего или второго объекта доступа (в случае логики «Доступ только вдвоём»).
  - «Доступ разрешён» - идентифицированному объекту доступа разрешён доступ.
  - «Доступ запрещён» - идентифицированному объекту доступа запрещён доступ.
  - «Ожидание алкотестирования» - для идентифицированного объекта доступа применяется режим с установленной опцией «Тестирование на алкоголь», идёт ожидание результата тестирования.

### 6.1.3. Стандартные профили индикации считывателя

В программе «Клиент» предусмотрены стандартные профили индикации с заранее установленными реакциями на определённые события, которые можно загрузить на считыватель Sigur.

В зависимости от того, по какому интерфейсу связи подключён считыватель и к какому контроллеру (к контроллеру Sigur или к контроллеру стороннего производителя), выбирается соответствующий профиль.

Если необходимо настроить индикацию на считывателе, подключённом к любому контроллеру (Sigur или стороннему) контроллеру **по Wiegand**, то на считыватель можно загрузить такие стандартные профили индикации как:

- Стандартный профиль Sigur MR100;
- Sigur MR, Wiegand (eng). Индикация сопровождается голосовой озвучкой на английском языке;
- Sigur MR, Wiegand (rus). Индикация сопровождается голосовой озвучкой на русском языке.

Если необходимо настроить индикацию на считывателе, подключённом к **контроллеру Sigur по OSDP**, то на считыватель можно загрузить такие стандартные профили индикации как:

- Sigur MR100, SSDP (eng). Индикация сопровождается голосовой озвучкой на английском языке;
- Sigur MR100, SSDP (rus). Индикация сопровождается голосовой озвучкой на русском языке.

Если необходимо настроить индикацию на считывателе, подключённом к

**контроллеру стороннего производителя по OSDP**, то на считыватель можно загрузить стандартный профиль – Sigur MR, OSDP.

Если же возникает необходимость изменить стандартный профиль или создать свой собственный, то с настройкой пользовательской индикации можно ознакомиться в соответствующем [разделе](#).

## 6.2. Настройка пользовательской индикации считывателя



Световая и звуковая индикация считывателей Sigur MR100 может быть гибко настроена только средствами ПО Sigur. Если считыватель настраивается на работу с контроллером СКУД стороннего производителя, то для настройки достаточно [бесплатной версии ПО](#).

Настройка индикации считывателей, подключённых **по Wiegand к любому контроллеру** (стороннего производителя или Sigur), а также для считывателей, подключённых **по OSDP к контроллеру стороннего производителя** производится следующим образом:

1. С помощью ПО Sigur «Клиент» создаётся профиль индикации. В окне настроек загружаются звуки и создаются реакции считывателя на какое-либо событие из списка. Создание профиля индикации более подробно рассматривается [ниже](#).
2. После окончательной настройки профиль либо прикрепляется к письму и отправляется на указываемый вами e-mail средствами ПО Sigur, либо сохраняется на компьютер, а далее передаётся на смартфон альтернативными способами.
3. Полученный профиль индикации открывается на смартфоне в приложении «Настройки», после чего загружается на считыватель по беспроводной технологии BLE. Подробнее этот процесс описан в разделе [«Загрузка профиля индикации на считыватель»](#).

Настройка индикации считывателей, подключённых **по OSDP к контроллеру Sigur** дополнительно может осуществляться альтернативным способом - профиль индикации можно загружать на считыватель централизованно из программы «Клиент» по протоколу SSDP. Подробнее этот способ описан в соответствующем [разделе](#).

Все действия, связанные с настройкой профилей индикации считывателя, производятся в меню «Файл - Настройки - Индикация».

Данное окно имеет 5 вкладок:



- Профили – содержит список профилей индикации. По умолчанию в нём созданы стандартные профили.

В данной вкладке создаются новые профили индикации: назначается индикация считывателя для режима ожидания, т.е. для «состояния покоя», а также указывается реакция на какое-либо событие из списка.

- Реакции считывателей Sigur – содержит список ранее настроенных реакций, а также стандартные реакции считывателя.

В данной вкладке создаются новые реакции считывателя характерные только для считывателей Sigur: настраивается логика световой и звуковой индикации. Эти реакции могут быть использованы при управлении индикацией считывателя как по какому-либо из трех его цифровых входов, так и по протоколу SSDP.

- Реакции OSDP - одержит список ранее настроенных реакций OSDP.

В данной вкладке создаются реакции считывателя, характерные для стандартного протокола OSDP и применимые для считывателей, управление индикацией которых может выполняться с помощью команд OSDP: указывается тип световой и параметры стандартной звуковой индикации считывателя.

- Звуки – содержит список ранее загруженных звуков и стандартные звуки.

В данной вкладке можно загрузить звук из файла, а также прослушать ту или иную запись из списка. Впоследствии звуки можно использовать при настройке реакций считывателей Sigur.

### 6.2.1. Создание профиля индикации считывателя

Для добавления нового профиля индикации считывателя перейдите во вкладку «Файл - Настройки - Индикация - Профили». Новый профиль индикации создаётся путём нажатия кнопки «+» или копированием другого профиля соответствующей кнопкой.

Имя профиля индикации может быть изменено в поле «Название». После изменения имени необходимо нажать «Применить».

Также при создании пользовательского профиля индикации необходимо выбрать его тип.

Тип показывает как именно будет осуществляться управление индикацией (по трём цифровым входам, по протоколу OSDP или по протоколу SSDP), для какого считывателя (Sigur или стороннего производителя) и при взаимодействии с каким контроллером (Sigur или стороннего производителя) настраивается данный профиль индикации. В зависимости

от того, какой тип был выбран, меняется список событий, на которые можно настроить реакции.



Например, если создаётся профиль индикации с типом «считыватель и контроллер Sigur», то наиболее полный функционал профиля данного типа можно будет получить, подключив считыватель к контроллеру по интерфейсу OSDP, а не Wiegand.

В частности, при подключении считывателя Sigur по интерфейсу OSDP есть возможность использовать не только реакции на события считывателя, но и реакции на события контроллера.

Если считыватель Sigur подключён к контроллеру по Wiegand, а управление индикацией происходит по трём линиям, то актуальна будет лишь часть функций, то есть можно будет настроить реакции на события считывателя, а реакции на события контроллера в таком случае не будут использоваться совсем.

При создании профиля индикации для считывателя Sigur можно выбрать один из следующих типов:

- Считыватель Sigur (Wiegand), сторонний контроллер – если считыватель подключён по Wiegand к контроллеру стороннего производителя и управление индикацией происходит по цифровым входам «IN1/GREEN», «IN2/RED» или «IN3/SOUND»;
- Считыватель и контроллер Sigur – если считыватель подключён к контроллеру Sigur независимо от интерфейса подключения. В случае подключения по интерфейсу Wiegand будут использоваться только реакции на события считывателя, а в случае подключения по интерфейсу OSDP для настройки реакции будут доступны все реакции (события считывателя и контроллера);
- Считыватель Sigur (OSDP), сторонний контроллер – если считыватель подключён к стороннему контроллеру по OSDP, и управление индикацией происходит посредством команд стандартного протокола OSDP.

Профили Реакции считывателей SIGUR Реакции OSDP Звуки

Название: Новый профиль  
 Тип: Считыватель и контроллер Sigur  
 Индикация состояния покоя  
 Тип: постоянный свет  
 Цвет: ■

События считывателя

Событие	Реакция	Приоритет
IN1/GREEN не активно	Без реакции	0 (Наименьший)
IN1/GREEN активно	Разрешение доступа 2	15
IN2/RED не активно	Без реакции	0 (Наименьший)
IN2/RED активно	Запрет доступа 2	15
IN3/SOUND не активно	Без реакции	0 (Наименьший)
IN3/SOUND активно	Считыватель не в норме	14
Считыватель на стене	Без реакции	0 (Наименьший)
Считыватель оторван	Вскрытие корпуса	14
Прочитан идентификатор	Без реакции	0 (Наименьший)
Температура вне нормы	Считыватель не в норме	14
Напряжение питания вне нормы	Считыватель не в норме	14

События контроллера

Событие	Реакция	Приоритет
Ожидание прохода	Без реакции	0 (Наименьший)
Взлом	Взлом	16
Удержание двери	Удержание двери	14
Тревога охранного шлейфа	Без реакции	0 (Наименьший)
Ожидание санкции оператора	Ожидание санкции оператора	14
Ожидание PIN-кода	Ожидание PIN-кода (rus)	14

отправить email применить отменить

OK Отмена

Создание и настройка нового профиля индикации считывателя.

Профиль индикации позволяет настроить:

1. Световую индикацию ожидания считывателем наступления какого-либо события.

Параметр «Тип индикации» может иметь следующие значения:

- «Постоянный свет» - цвет светодиода не меняется до наступления какого-либо события.
- «Мигание» - считыватель периодически изменяет цвет светодиода: сначала включается «Цвет 1» на указанное время, затем включается «Цвет 2» на соответствующее настройке время.

2. Реакцию считывателя на какое-либо событие.

Реакции, созданные на вкладках «Реакции считывателей Sigur», могут быть назначены на одну из представленных ниже функций.

**Полный перечень функций на вкладке «Профили».**

<b>Название функции</b>	<b>Описание. Реакция активируется при:</b>
IN1/GREEN не активно	Линия IN1/GREEN не замкнута на GND.
IN1/GREEN активно	Линия IN1/GREEN замкнута на GND.
IN2/RED не активно	Линия IN2/RED не замкнута на GND.
IN2/RED активно	Линия IN2/RED замкнута на GND.
IN3/SOUND не активно	Линия IN3/SOUND не замкнута на GND.
IN3/SOUND активно	Линия IN3/SOUND замкнута на GND.
Считыватель на стене	Считыватель закреплён на настенной панели.
Считыватель оторван	Считыватель извлечён из настенной панели.
Прочитан идентификатор	Чтение идентификатора считывателем (карта или смартфон).
Температура вне нормы	Выход температуры считывателя за пределы нормы.
Напряжение питания вне нормы	Напряжение считывателя вышло за пределы нормы.
Ожидание прохода	Объекту доступа был разрешён доступ, контроллер ожидает, когда объект доступа совершит проход.
Взлом	Было зафиксировано пересечение точки доступа несанкционированным образом, например, активировался датчик открытия двери.
Удержание двери	Датчик открытия двери не возвращён в нормальное состояние до истечения времени, установленного в настройках точки доступа параметром «Время до сигнала «Удержание двери»».
Тревога охранного шлейфа	От охранного шлейфа контроллера Sigur (E2, E4) поступило событие «Тревога».
Ожидание санкции оператора	Для идентифицированного объекта доступа применяется режим с установленной опцией «Требовать санкции оператора на проход», идёт ожидание решения оператора.

Название функции	Описание. Реакция активируется при:
Ожидание PIN-кода	Для идентифицированного объекта доступа применяется режим с установленной опцией «Дополнительно запрашивать PIN код», контроллер ожидает получения кода от подключенной кодонаборной панели.
Ожидание второй карты	Для идентифицированного объекта доступа применяется режим с установленной опцией «Доступ в сопровождении» или «Доступ только вдвоём», идёт ожидание идентификации сопровождающего или второго объекта доступа (в случае с опцией «Доступ только вдвоём»).
Доступ разрешён	Идентифицированному объекту доступа разрешён доступ.
Доступ запрещён	Идентифицированному объекту доступа запрещён доступ.
Ожидание алкотестирования	Для идентифицированного объекта доступа применяется режим с установленной опцией «Тестирование на алкоголь», идёт ожидание результата тестирования.

3. Приоритет - параметр, определяющий, сменится ли индикация реакции при наступлении другой реакции. Реакции могут быть двух типов:  
**1** - длительность реакции определяется длительностью события (Сменить цвет, мигание непрерывно);  
**2** - фиксированная длительность реакции (Мигнуть однократно, мигнуть один раз).

**Смена реакций в зависимости от их приоритетов и типов.**

Тип реакции		Приоритет текущей реакции	Результат. Наступающая реакция:
Текущей	Наступающей		
1	1	Меньше или равен	Перекрыт текущую
		Больше	Не перекрыт текущую
1	2	Любой	Перекрыт текущую

Тип реакции		Приоритет текущей реакции	Результат. Наступающая реакция:
Текущей	Наступающей		
2	1	Меньше или равен	Перекроет текущую
		Больше	Не перекроет текущую
2	2	Любой	Перекроет текущую

Опционально может быть настроен «приоритет системных событий в Sigur MR». Этот параметр будет актуален только для тех случаев, когда считыватель подключён к контроллеру по интерфейсу OSDP, и управление индикацией происходит стандартными командами OSDP. В качестве системных событий выступают события, переданные контроллером на считыватель. Таким образом настройкой данного параметра можно определить приоритет событий, генерируемых контроллером, над событиями, генерируемыми считывателем.

После настройки профиля индикации необходимо нажать «Применить».

## 6.2.2. Создание реакции считывателя

Для добавления новой реакции считывателя Sigur на определенное событие перейдите во вкладку «Файл - Настройки - Индикация - Реакции считывателей Sigur». Новая реакция создаётся путём нажатия кнопки «+» или копированием другой реакции соответствующей кнопкой.

Имя реакции задаётся в поле «Название». После изменения имени необходимо нажать «Применить».

Создание реакции для считывателя Sigur.

Реакция содержит следующие основные элементы:

1. Тип индикации - определяет тип световой индикации считывателя на событие. Тип световой индикации может быть:

- «Без реакции» – световая индикация на событие отсутствует. Цвет светодиода не будет изменён.
- «Мигнуть однократно»<sup>2</sup> – считыватель меняет цвет светодиода на «Цвет 1» на указанное время.
- «Мигание несколько раз»<sup>2</sup> – считыватель периодически изменяет цвет светодиода: сначала включается «Цвет 1» на указанное время, затем включается «Цвет 2» на соответствующее настройке время. Последовательность повторяется установленное количество раз.
- «Сменить цвет»<sup>1</sup> – считыватель изменяет цвет светодиода на «Цвет 1».
- «Мигание непрерывно»<sup>1</sup> – считыватель периодически изменяет цвет светодиода: сначала включается «Цвет 1» на указанное время, затем включается «Цвет 2» на соответствующее настройке время.

2. Тип звука - определяет тип звуковой индикации считывателя на событие.

Типы звуковой индикации могут быть следующими:

- «Нет звука» – звуковая индикация на событие отсутствует.
- «Широкополосный» – воспроизводится один из пользовательских звуков вкладки «Звуки».

Звук воспроизводится либо установленное число раз<sup>2</sup>, либо непрерывно<sup>1</sup>. В обоих случаях может быть установлен интервал пауз.

(<sup>1</sup>) – Длительность реакции определяется длительностью события.

(<sup>2</sup>) – Фиксированная длительность реакции.

После внесения изменений в настройки реакции необходимо нажать «Применить».

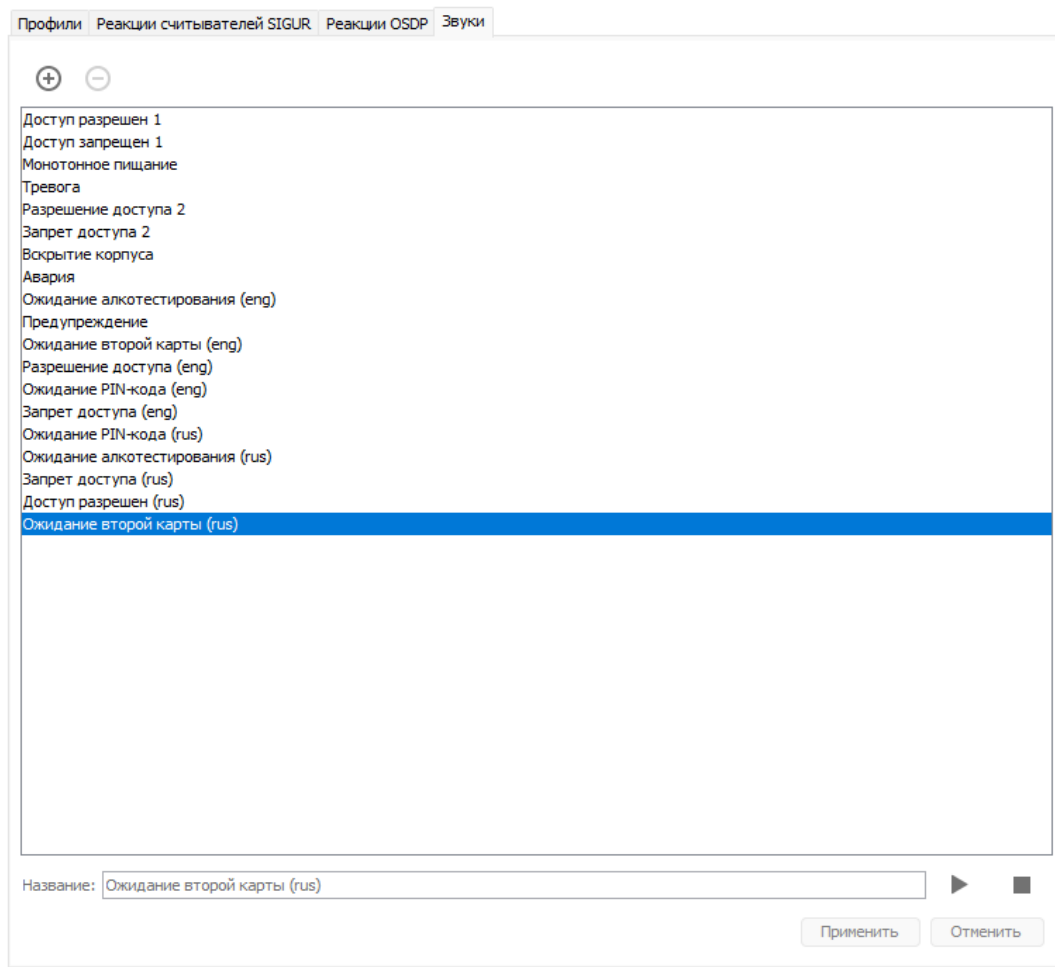
### 6.2.3. **Добавление звука реакции считывателя**

Для загрузки нового звукового файла в ПО перейдите во вкладку «Файл - Настройки - Индикация - Звуки». Нажмите на кнопку «+» сверху. В открывшемся окне выберите нужный вам файл формата .wav, .aiff или .au.

Имя звука задаётся в поле «Название». После изменения имени необходимо нажать «Применить».

В этой же вкладке вы можете прослушать любой звук из списка, нажав соответствующие кнопки воспроизведения в нижнем правом углу.





Вкладка «Звуки» в окне «Файл - Настройки - Индикация».

#### 6.2.4. Способы загрузки пользовательского профиля индикации на считыватель

Пользовательский профиль индикации можно загрузить на считыватель двумя способами:

1. Загрузить конфигурационный файл индикации с помощью приложения «Настройки», установленного на Android- смартфоне. Подробно этот способ описан в соответствующем [разделе](#).
2. Загрузить профиль индикации с помощью программы «Клиент» через OSDP интерфейс.

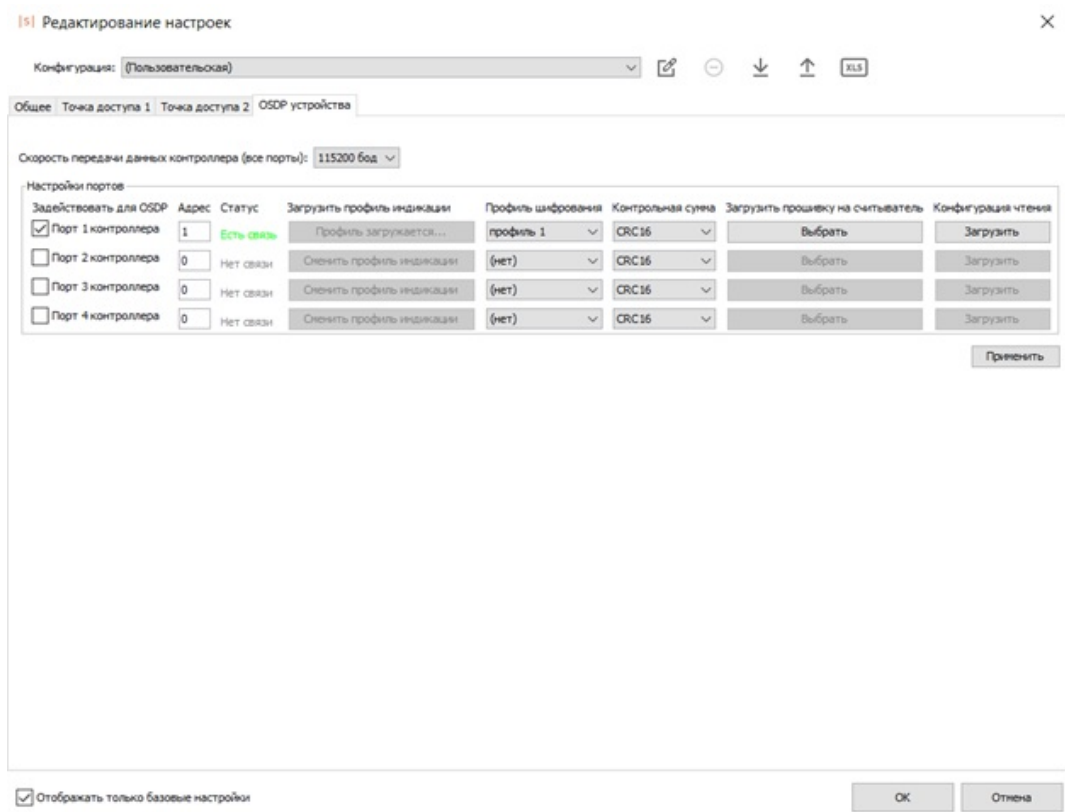


Этот способ актуален только для тех случаев, когда считыватель Sigur подключен к контроллеру Sigur по интерфейсу OSDP, иными словами данная возможность - отличительная особенность протокола SSDP, позволяющая централизованно с рабочего места обновить профиль индикации на считывателях.

- Для этого в программе «Клиент» на вкладке «Оборудование» можно перейти в меню настроек точки доступа, а далее в новом окне на вкладку «OSDP устройства», после чего для конкретного порта контроллера нажать кнопку «Сменить профиль индикации», выбрать из выпадающего списка профиль индикации, который необходимо загрузить на считыватель, и нажать кнопку «Применить». После этих действий начнётся процесс загрузки профиля индикации на считыватель.

Загрузка профиля индикации происходит в фоновом режиме и может занимать продолжительное время.

Во время загрузки кнопка «Сменить профиль индикации» будет изменена на информационное сообщение «Профиль загружается» и будет неактивна, а в журнале системных событий (подробнее можно ознакомиться в разделе «**Журнал системных событий**») появится событие «Начало загрузки профиля индикации на считыватель».



Процесс загрузки профиля индикации на считыватель через программу «Клиент».

- При успешной загрузке профиля индикации кнопка «Сменить профиль индикации» снова станет активной, а в журнале системных событий появится событие «Профиль индикации успешно загружен на считыватель».
- При неуспешной загрузке профиля индикации в журнале системных событий появится событие об ошибке. Подробнее ознакомиться с возможными ошибками можно в соответствующем разделе.

## 7. Настройка реакции на вскрытие корпуса считывателя

При открытии и закрытии корпуса считывателя на управляющий контроллер отправляются специальные посылки в формате Wiegand-58.

По приходу на сервер данных посылок можно настроить какую-либо реакцию системы.



Если считыватель подключён к стороннему контроллеру, то для настройки обратитесь к документации данной системы.

При подключении считывателя к контроллерам Sigur можно настроить реакцию системы, используя дополнительный модуль «Реакция на события». В качестве данной реакции могут выступать: отправка уведомления, блокировка точек доступа и т.п.

Пример настроек:

- В программе «Клиент» создайте две новых учётных карточки пользователя с любыми именами, например: «Открытие корпуса считывателя» и «Закрытие корпуса считывателя».
- У пользователя «Открытие корпуса считывателя» в поле «Пропуск» установите W58 и значение, равное «FFFFFFFFFFFF00» (без кавычек). У учётной записи «Закрытие корпуса считывателя» сделайте аналогично со значением, равным «FFFFFFFFFFFF01».
- Удалите все точки доступа у данных пользователей на вкладке «Общее».
- Перейдите во вкладку «События», создайте новое событие кнопкой «Добавить событие».
- В пункте «Редактирование события» установите тип события: «По факту запрета доступа».
- Объект доступа – «Открытие корпуса считывателя» и/или «Закрытие корпуса считывателя».
- Выберите точки доступа из списка, к которым подключены считыватели Sigur. Укажите фиксируемые направления («Вход», «Выход»).
- В пункте «Редактирование реакции на событие» выберите необходимую вам реакцию:
  - установить режим точек доступа;
  - уведомить оператора;
  - отправлять SMS/PUSH/Telegram сообщение;
  - отправлять e-mail;
  - осуществлять HTTP-запрос;
  - выполнить команду ОС.

Пример настройки того или иного типа реакции на событие приведён в документе «Руководство пользователя ПО Sigur».

## 8. Программирование считывателей



Программирование считывателей Sigur на текущий момент производится только средствами ПО Sigur. Вы можете воспользоваться любой актуальной версией нашего ПО, в том числе бесплатной. Дистрибутив доступен на нашем [официальном сайте по ссылке](#).

Программирование считывателей Sigur осуществляется в 3 этапа:

- настройка параметров считывателя через ПО «Клиент»;
- запись данных конфигурации на карту или в файл;
- непосредственное программирование считывателя на настроенную конфигурацию.

После установки ПО откройте программу «Клиент» и перейдите во вкладку «Файл – Настройки – Бесконтактная идентификация».

В этой вкладке возможно изменение следующих параметров считывателя:

- Разрядность Wiegand-выхода. Поддерживаются форматы Wiegand-26, 34 и 58;
- Параметры работы считывателя с картами (чтение UID или защищенный режим работы, порядок следования байт для карт Mifare Classic 1K/4K и Mifare Plus). Для защищённого режима указываются реквизиты доступа к памяти карты;
- Параметры работы считывателей Sigur со смартфонами: «Базовый» или «Пользовательский» режим, секретный ключ доступа, дальность срабатывания и политика чтения смартфонов;
- Сервисный пароль считывателя.

Подробное описание каждого пункта настройки представлено в следующих разделах:

- [Работа с картами Mifare](#)
- [Работа с банковскими картами](#)
- [Работа со смартфонами](#)

После того, как вы примените данные параметры, конфигурацию необходимо будет записать на считыватели вручную. Для считывателей Sigur доступно 3 способа, как это сделать:

- [Программирование считывателя мастер-картой](#)

- [Программирование считывателя конфигурационным файлом](#)
- [Программирование считывателя через протокол SSDP](#)

## 8.1. Программирование считывателя мастер-картой



Данный способ доступен для всех считывателей Sigur.

Для настройки считывателя предварительно необходимо создать мастер-карту. Вам потребуется:

- Карта Mifare Classic 1K/4K или Mifare Plus в транспортной конфигурации, т.е. «чистая».
- Настольный USB-считыватель модели ACR 1252U.
- ПО Sigur с официального сайта. Для настройки подойдёт [Бесплатная версия](#).

Перечень доступных для программирования параметров и порядок их настройки представлен в разделе [«Программирование считывателя»](#).

После установки всех параметров работы считывателя в ПО «Клиент», в разделе «Файл – Настройки – Бесконтактная идентификация» нажмите на кнопку «Эмиссия мастер-карты Sigur». Поднесите любую чистую карту (Mifare Classic 1K/4K или Mifare Plus) к настольному считывателю. Программа уведомит вас о результате операции.



Для создания Mifare Plus мастер-карты Sigur с иными параметрами понадобится другая «чистая» карта!

Если считыватель был запрограммирован ранее, то сначала нужно произвести его аппаратный сброс. Процесс описан в разделе [«Аппаратный сброс»](#).

Если считыватель Sigur не был запрограммирован ранее, или вы уже произвели его аппаратный сброс, то:

- выключите и включите считыватель;
- поднесите мастер-карту к считывателю (время ожидания считывателем мастер-карты равно 25 секундам).

После поднесения мастер-карты считыватель издаст характерный звук.

## 8.2. Программирование считывателя конфигурационным файлом



Данный способ доступен для всех считывателей Sigur.

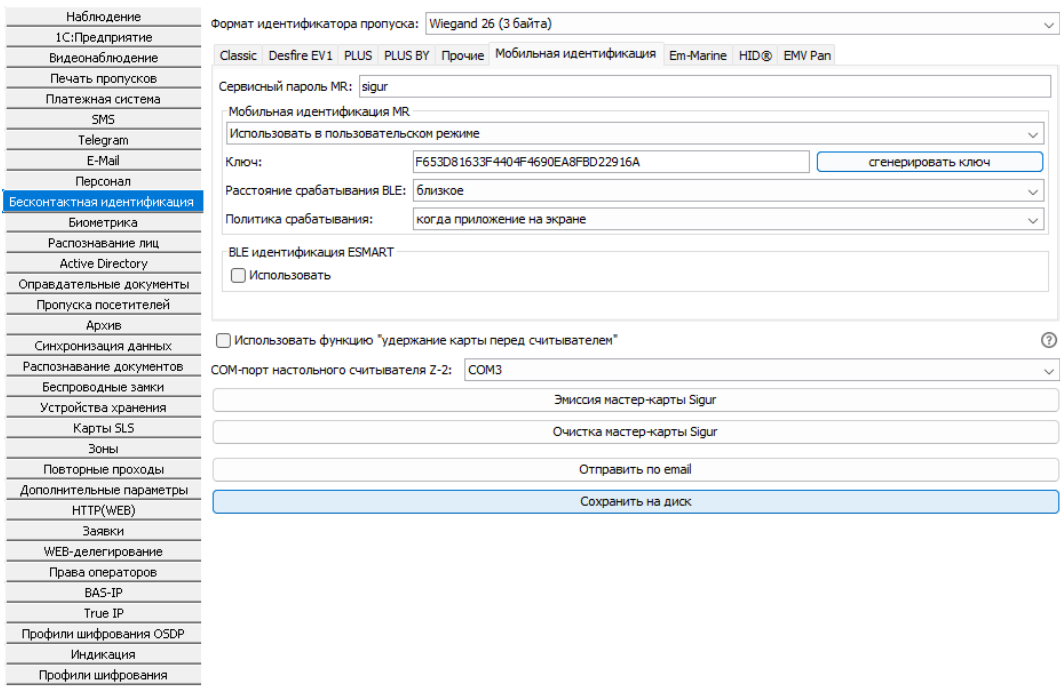
Для программирования считывателя конфигурационным файлом вам потребуется:

- Смартфон с ОС Android с установленным приложением «Настройки» с доступом к какому-либо почтовому ящику и с поддержкой функции BLE;
- Опционально: доступ к альтернативному почтовому ящику, с которого будет отправлен файл конфигурации средствами ПО Sigur. Файл конфигурации может быть передан на смартфон альтернативными способами (через мессенджеры/флеш-накопитель и пр.);
- ПО Sigur с официального сайта. Для настройки подойдёт бесплатная версия.

Перечень доступных для программирования параметров и порядок их настройки представлен в разделе «Программирование считывателя».

Файл конфигурации можно сохранить на компьютер для последующей передачи на смартфон. Для этого в ПО «Клиент» в меню «Файл - Настройки - Бесконтактная идентификация» есть соответствующая кнопка «Сохранить на диск», после нажатия на которую программа предложит выбрать директорию для сохранения файла и при необходимости изменить название файла. Далее файл можно, например, отправить на телефон через мессенджер (Telegram, Viber и пр.).





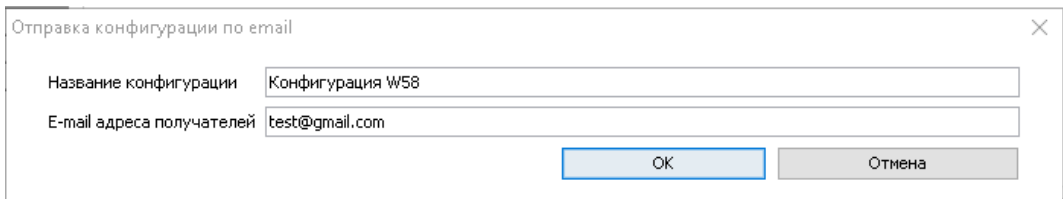
Кнопка «Сохранить на диск» в меню «Файл - Настройки - Бесконтактная идентификация».

Также можно воспользоваться альтернативным способом передачи файла на телефон - отправить на email непосредственно из ПО Sigur. Для отправки письма с конфигурационным файлом серверу Sigur потребуется доступ к серверу исходящей почты. Подробная инструкция по настройке реквизитов доступа сервера исходящей почты представлена в разделе [«Настройка параметров сервера исходящей почты»](#).

i

Этот способ будет более предпочтителен пользователям, у которых уже настроен доступ к серверу исходящей почты.

После установки всех параметров работы считывателя в ПО «Клиент», в разделе «Файл – Настройки – Бесконтактная идентификация» нажмите кнопку «Отправить по e-mail». В открывшемся меню введите название любое конфигурации и укажите почтовый ящик, на который будет выслан файл конфигурации. Нажмите «ОК».



Окно отправки конфигурации по email.

После получения файла конфигурации на смартфоне любым из описанных выше способов для дальнейшего программирования считывателя следуйте пунктам раздела «[Загрузка профиля конфигурации на считыватель](#)».

### 8.3. Программирование считывателя через протокол SSDP



Этот способ актуален только для тех случаев, когда считыватель Sigur подключён к контроллеру Sigur по интерфейсу OSDP, иными словами данная возможность - отличительная особенность протокола SSDP, позволяющая централизованно с рабочего места обновить конфигурацию чтения на считывателях.

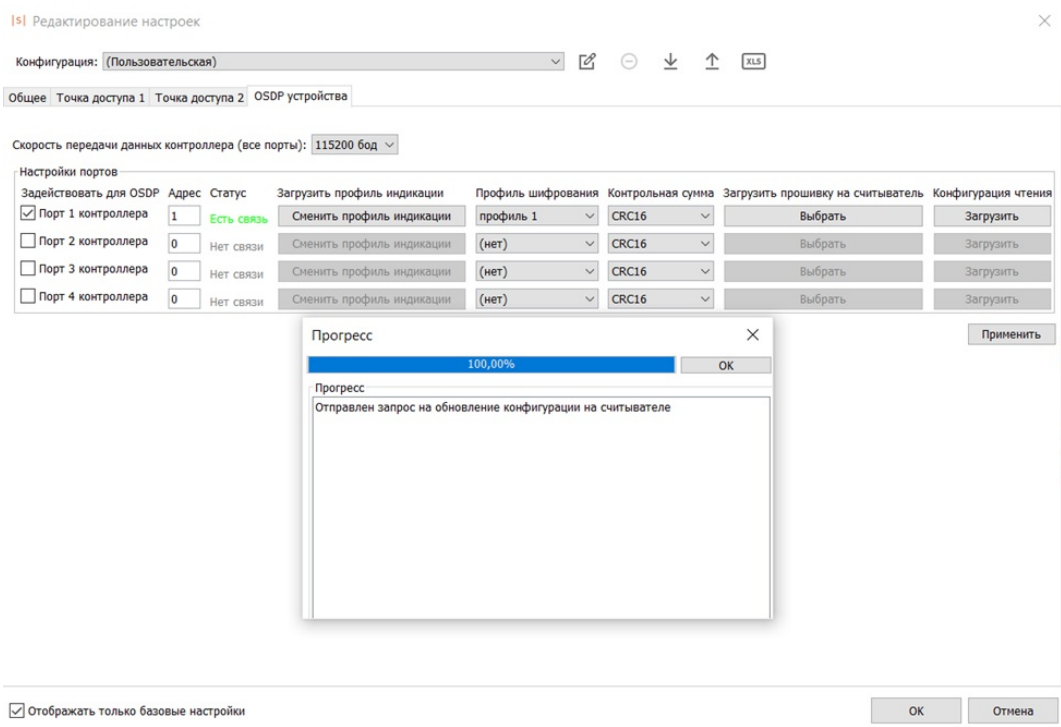
Также необходимо соблюсти следующие технические требования:

- версия микропрограммы считывателя должна быть не ниже 43;
- версия микропрограммы контроллера должна быть не ниже 18;
- версия ПО должна быть не ниже 1.1.1.48s.

Для программирования считывателей потребуется ПО Sigur, подойдёт [бесплатная версия](#).

Загрузка конфигурации чтения на считыватель будет осуществляться через ПО «Клиент». Процесс состоит из нескольких шагов:

- В меню «Файл-Настройки-Бесконтактная идентификация» настроить необходимые параметры считывателя. Более подробно про настройку параметров можно посмотреть в разделе «[Программирование считывателей](#)». Когда все необходимые параметры будут настроены, нажать на кнопку «ОК», чтобы все внесённые изменения применились;
- На вкладке «Оборудование» необходимо установить связь с контроллером Sigur (E2 или E4), к которому по интерфейсу OSDP подключён считыватель.
- В меню настроек точки доступа на вкладке «OSDP устройства» для конкретного порта контроллера нажать кнопку «Загрузить» в блоке «Конфигурация чтения». Начнется процесс загрузки конфигурации чтения на считыватель;
- По окончании процесса загрузки конфигурации на считыватель необходимо нажать на кнопку «ОК» в окне прогресса обновления. Результат загрузки конфигурации чтения на считыватель протоколируется в журнале системных событий, подробнее о котором можно прочитать в соответствующем [разделе](#).



Окно прогресса обновления конфигурации чтения на считывателе.

## 9. Сброс параметров считывателя к заводским настройкам

Ниже следует описание способов сброса параметров считывателя. Для считывателей доступно 2 способа сброса параметров считывателя к заводским настройкам:

1. Аппаратный сброс.
2. Сброс параметров через приложение «Настройки».

Оба способа позволяют сбросить следующие параметры считывателя:

1. Разрядность Wiegand.
2. Параметры работы считывателя с картами.
3. Параметры работы считывателя со смартфонами.
4. Сервисный пароль считывателя.

Далее представлены способы сброса параметров считывателя к заводским настройкам.

### 9.1. Аппаратный сброс



Все считыватели Sigur поддерживают функцию аппаратного сброса на заводские настройки.

Для аппаратного сброса настроек считывателя необходимо:

1. Отключить питание считывателя.
2. Замкнуть между собой зеленый (Data 0) и жёлтый (Beep) провода.
3. Подать питание на считыватель, после чего разъединить провода.

Если считыватель был ранее запрограммирован, то при успешном сбросе он издаст характерный звуковой сигнал.

### 9.2. Сброс параметров считывателя через приложение «Настройки»

Все считыватели Sigur поддерживают функцию сброса на заводские настройки через приложение «Настройки».

Для сброса параметров чтения карт и смартфонов, а также разрядности Wiegand следуйте пунктам раздела «Сброс конфигурации чтения»

считывателя».

Для сброса параметров индикации следуйте пунктам раздела «Сброс конфигурации индикации считывателя».

### 9.3. Параметры работы считывателя по умолчанию

При первом включении, а также после сброса конфигурации чтения считыватель имеет следующие настройки:

#### Параметры работы считывателя по умолчанию.

Название параметра	MR100 Lite	MR100	MR100 Multi
Выход	Wiegand-26		
Чтение карт Mifare (Ultralight, Classic, Mini, ID, DESFire, Plus)	UID (прямой порядок байт)		
Чтение прочих карт стандарта ISO14443-A	UID		
Чтение PAN-номера банковской карты	-	Отключено	
Работа считывателя со смартфонами	-	«Базовый» режим работы, дальность чтения – «Близко» и режим работы – «Когда приложение на экране»	
Чтение карт EM Marine и HID ProxCard II	-	-	Включено, фиксированный facility - не используется
Сервисный пароль считывателя	sigur		

## 10. Настройка доступа ПО Sigur к почтовым серверам

Настройка доступа ПО Sigur к почтовым серверам может понадобиться, если вы используете какую-либо из данных функций:

- Доступ по смартфону: отправка приглашающих писем и регистрация идентификаторов смартфонов в системе.
- Загрузка на считыватель файла конфигурации чтения идентификаторов.
- Загрузка на считыватель файла конфигурации индикации.

### 10.1. Настройка параметров сервера исходящей почты

Вы можете использовать как SMTP сервер вашей организации, так и любой другой, в том числе бесплатный.

Перейдите в программе «Клиент» в меню «Файл – Настройки – E-mail». Заполните поля подпункта «Почтовый сервер для отправки исходящих писем»:


- «Адрес SMTP-сервера» – адрес используемого для отправки писем почтового сервера.
- «Порт SMTP сервера» – порт для подключения к почтовому серверу.
- «От кого» – e-mail адрес отправителя.
- «Использовать аутентификацию» – включает использование аутентификации на почтовом сервере.
- «SMTP логин» – логин для аутентификации на SMTP сервере.
- «SMTP пароль» – пароль для аутентификации на SMTP сервере.
- «Использовать SSL» – включает использование криптографического протокола для обеспечения более безопасной связи.

После указания реквизитов вы можете проверить правильность настройки, нажав кнопку «Сохранить параметры и протестировать». Укажите e-mail адрес получателя и нажмите ОК.

Если всё введено верно, вы увидите сообщение «Письмо успешно отправлено». Убедитесь в факте его получения на указанном вами почтовом ящике.

### 10.2. Настройка параметров сервера входящей почты

Сервер входящей почты необходим для приёма сервером СКУД писем, отправленных со смартфонов, для их автоматического внесения в список идентификаторов пользователя. Вы можете использовать как сервер вашей организации, так и любой бесплатный. Адреса серверов исходящей и входящей почты могут отличаться.



Для нужд СКУД требуется завести отдельный почтовый ящик. Письма в почтовом ящике будут УДАЛЕНЫ сервером СКУД.

- «Сервер» – адрес почтового сервера.
- «Порт» – входящий порт почтового сервера.
- «Протокол» – протокол работы сервера входящей почты. Доступны варианты «IMAP» и «POP».
- «Логин» – логин для аутентификации на сервере входящей почты.
- «Пароль» – пароль для аутентификации на сервере входящей почты.
- «E-mail» – укажите адрес электронной почты. На указанный вами адрес будут приходить ответные письма от пользователей.
- «Использовать SSL» – включает использование криптографического протокола для обеспечения более безопасной связи.

|s| Редактирование настроек
×

Наблюдение	Почтовый сервер для отправки исходящих писем:
Видеонаблюдение	Адрес SMTP сервера: <input type="text" value="smtp.gmail.com"/>
E-Mail	Порт SMTP сервера: <input type="text" value="465"/>
Персонал	От кого: <input type="text" value="test.sigur.stand@gmail.com"/>
Active Directory	<input checked="" type="checkbox"/> Использовать аутентификацию:
Архив	SMTP логин: <input type="text" value="test.sigur.stand@gmail.com"/>
Биометрика	SMTP пароль: <input type="password" value="....."/>
Беспроводные замки	<input checked="" type="checkbox"/> Использовать SSL
Устройства хранения	Сохранить параметры отправки e-mail и протестировать
Mifare и BLE	Почтовый сервер для получения входящих писем:
Зоны	Сервер: <input type="text" value="imap.gmail.com"/>
Повторные проходы	Порт: <input type="text" value="993"/>
Дополнительные параметры	Протокол: <input type="text" value="IMAP"/>
Распознавание лиц	Логин: <input type="text" value="test.sigur.stand@gmail.com"/>
HTTP(WEB)	Пароль: <input type="password" value="....."/>
WEB-делегирование	E-mail: <input type="text" value="test.sigur.stand@gmail.com"/>
Пароли	<input checked="" type="checkbox"/> Использовать SSL
Индикация	

Окно настройки параметров почтового сервера.

## 11. Работа с картами Mifare

### 11.1. Работа в незащищённом режиме, чтение UID

Для карт Mifare поддерживается функция считывания их открытого уникального идентификатора – UID.

По умолчанию считыватель настроен на чтение UID карты и выдаёт его в прямом порядке байт в формате Wiegand-26. Вы можете изменить выходной формат Wiegand на другой.

Для этого:

- В программе «Клиент» перейдите в меню «Файл - Настройки». Выберите пункт «Бесконтактная идентификация». Установите сверху пункт «Формат идентификатора пропуска» равным одному из следующих вариантов: Wiegand-26 (3 байта), Wiegand-34 (4 байта) или Wiegand-58 (7 байт). Эта настройка предназначена как для конфигурации выходного формата считывателя, так и для настройки формата получаемых номеров карт с настольного считывателя.
- Если дальнейших настроек считывателя не требуется, то следуйте пунктам раздела «Программирование считывателя мастер-картой» или «Программирование конфигурационным файлом».

### 11.2. Работа в защищённом режиме

Считывателем поддерживается защищённый режим работы для карт Mifare Classic 1K/4K и Mifare Plus SL3, а также банковских карт МИР, Visa и MasterCard в режиме эмуляции карты Mifare Classic 1K/4K или Plus.

Другие режимы эмуляции карт Mifare не могут быть использованы для реализации защищённого режима работы и подойдут только для чтения их UID.

#### 11.2.1. Настройка работы с картами Mifare Classic 1K/4K

- В программе «Клиент» перейдите в меню «Файл – Настройки».
- Выберите пункт «Бесконтактная идентификация», вкладку «Classic».
- Установите значение «В качестве идентификатора пропуска использовать» равным «Данные из памяти (защищённый режим)».





Если у вас уже был выбран данный режим и использовались карты Mifare, то ни в коем случае не изменяйте реквизиты доступа системы к памяти карт. Это приведёт к тому, что новые карты не будут иметь доступ к старым считывателям, а старые — к новым. Придётся перезаписать все старые карты, используя новые реквизиты и перепрограммировать все остальные считыватели.

- «Номер блока памяти» (в шестнадцатеричном формате) в большинстве случаев значение достаточно оставить равным по умолчанию.
- «Ключ для доступа к памяти». Как правило, достаточно нажать кнопку «Сгенерировать ключ».
- «В память карты записывать» - выберите либо «Автосгенерированное значение», либо «UID карты». В большинстве случаев достаточно оставить равным по умолчанию.
- Если дальнейших настроек считывателя не требуется, то следуйте пунктам раздела «Программирование считывателя мастер-картой» или «Программирование конфигурационным файлом».

### 11.2.2. Настройка работы с картами Mifare Plus

- В программе «Клиент» перейдите в меню «Файл - Настройки».
- Выберите пункт «Бесконтактная идентификация», вкладку «PLUS».
- Выберите ваш тип карты: PLUS S или PLUS X.
- Установите значение «В качестве идентификатора пропуска использовать» равным «Данные из памяти (защищённый режим)».



Если у вас уже был выбран данный режим и использовались эти карты Mifare, то ни в коем случае не изменяйте реквизиты доступа системы к памяти карт. Это приведёт к тому, что новые карты не будут иметь доступ к старым считывателям, а старые — к новым. Придётся перезаписать все старые карты, используя новые реквизиты и перепрограммировать все остальные считыватели.

- «Номер блока памяти» в шестнадцатеричном формате. В большинстве случаев значение достаточно оставить равным по умолчанию.
- «Ключ для доступа к памяти». Как правило, достаточно нажать кнопку «Сгенерировать ключ». Остальные поля заполнятся автоматически.
- «В память карты записывать» - выберите либо «Автосгенерированное значение», либо «UID карты». В большинстве случаев достаточно оставить равным по умолчанию.
- Если дальнейших настроек считывателя не требуется, то следуйте пунктам раздела «Программирование считывателя мастер-картой» или «Программирование конфигурационным файлом».

«Программирование конфигурационным файлом».

### 11.2.3. Правила заполнения служебных полей настроек карт Mifare

Заполняя служебные поля вручную, необходимо соблюдать следующие условия:

#### Для карт Mifare Classic 1K/4K:

- **«Номер блока памяти».**

В этой строке в шестнадцатеричном формате указывается номер блока памяти для хранения идентификатора пропуска. Указываемый блок не должен быть равен «0» (нулевой блок нулевого сектора) и не должен быть последним блоком сектора.

Для карт **Mifare Classic 1K** значение может быть 01h до 3Fh. Остаток от деления указываемого значения на 4 не должен равняться 3).

Для карт **Mifare Classic 4K** значение может быть 01h до FFh. Остаток от деления указываемого значения на 4 не должен равняться 3) для значений, меньших 80h. Остаток от деления на 16 не должен быть равен 15 для значений, начиная с 80h.

- **«Ключ для доступа к памяти».**

Поле для указания значения секретного ключа (KEY-A), используемого для доступа к указанному блоку памяти карты, в шестнадцатеричном формате. **Значение ключа для доступа к памяти по умолчанию («FFFFFFFFFFFF») не должно использоваться в защищённом режиме!**

Можно ввести собственное значение вручную или воспользоваться кнопкой «Сгенерировать ключ».

- **«В память карты записывать».**

Позволяет выбрать из выпадающего списка, что будет записано в память карты в качестве идентификатора. Доступно два варианта: UID карты или автоматически созданное значение. Формат записываемого значения будет соответствовать выбранному в верхней части окна «Формату идентификатора пропуска».

- **«Биты чётности Wiegand хранятся на карте».**

Данный параметр не используется считывателем и его значение должно оставаться равным по умолчанию, то есть отключено.

#### Для карт Mifare Plus:

- **«Номер блока памяти».**

Значение данного поля указывается в шестнадцатеричном формате, нумерация блоков начинается с 00h (недоступен и не может быть использован).

Для карт **Mifare Plus 2K** значение должно быть от 01h до 79h. Остаток от деления значения на 4 не должен быть равен трём.

Для карт **Mifare Plus 4K** значение должно быть от 01h до FFh. Остаток от деления значения на 4 не должен быть равен трём для значений, меньших 80h. Начиная с 80h остаток от деления значения на 16 не должен равняться 15.

- **«Ключ для доступа к блоку памяти».**

Поле для ввода AES ключа, используемого для доступа к указанному выше блоку памяти. Значение задаётся в шестнадцатеричном формате и должно состоять из 16 байт (32 символов). По умолчанию состоит из всех нулей и не должен использоваться в защищённом режиме с таким значением.

- **«Мастер-ключ карты».**
- **«Конфиг-ключ карты».**

Два поля для ввода AES ключей, используемых системой для персонализации карты. Значения задаются в шестнадцатеричном формате и должны состоять из 16 байт (32 символов).

- **«Ключ для переключения в SL2».**

Поле для ввода AES ключа, переключающего карту на более высокий уровень безопасности - Security Level 2. Используется системой в процессе персонализации карты. Значение задаётся в шестнадцатеричном формате и должно состоять из 16 байт (32 символов).

- **«Ключ для переключения в SL3».**

Поле для ввода AES ключа, переключающего карту на более высокий уровень безопасности - Security Level 3. Используется системой в процессе персонализации карты. Значение задаётся в шестнадцатеричном формате и должно состоять из 16 байт (32 символов).

- **«В память карты записывать:».**

Позволяет выбрать из выпадающего списка, что будет записано в память карты в качестве идентификатора. Доступно два варианта: UID карты или автосгенерированное значение. Формат записываемого значения будет соответствовать выбранному в верхней части окна «Формату идентификатора пропуска».

## 12. Работа с банковскими картами

### 12.1. Чтение UID или эмуляция Mifare банковской картой

Все модификации считывателей Sigur позволяют использовать в качестве идентификаторов бесконтактные банковские карты MasterCard, Visa, МИР в режиме чтения UID (при наличии статического UID), либо аналогично картам Mifare, если банковская карта умеет эмулировать Mifare.



Эмулирует ли банковская карта Mifare, и какой именно формат - необходимо уточнить напрямую у банка, выпустившего карту.

Для настройки считывателей на работу в данном режиме достаточно:

- В программе «Клиент» перейдите в меню «Файл - Настройки». Выберите пункт «Бесконтактная идентификация». Установите сверху пункт «Формат идентификатора пропуска» равным одному из следующих вариантов: Wiegand-26 (3 байта), Wiegand-34 (4 байта) или Wiegand-58 (7 байт). Эта настройка предназначена как для конфигурации выходного формата считывателя, так и для настройки формата получаемых номеров карт с настольного считывателя.
- Если банковская карта не эмулирует какую-либо карту из семейства Mifare, то в этом же меню перейдите на вкладку «Прочие» и поставьте галку «Использовать UID в качестве идентификатора пропуска».
- Если банковская карта эмулирует какую-либо карту из семейства Mifare:
  - Для чтения UID эмулируемой карты в этом же меню выберите вкладку, на которой указан формат ваших карт (Classic или Plus). Установите пункт «В качестве идентификатора пропуска использовать» равным «UID».
  - Для работы в защищённом режиме выполните настройки, описанные в разделе [«Работа с картами Mifare в защищённом режиме»](#).



У банка, выпустившего карту, необходимо уточнить номер блока памяти, который можно использовать для нужд СКУД, а также ключ от данного блока памяти, если он есть.

- Если дальнейших настроек считывателя не требуется, то следуйте

пунктам раздела «Программирование считывателя мастер-картой» или «Программирование конфигурационным файлом».

## 12.2. Чтение PAN-номера банковской карты

Модификации считывателей Sigur MR100 и Sigur MR100 Multi позволяют использовать в качестве идентификатора PAN-номер банковской карты, используя технологию EMV (Europay + MasterCard + VISA). Может использоваться как физическая карта, так и добавленная в электронный кошелек на смартфоне (МИР Pay, Google Pay, Apple Wallet, Samsung Pay). По факту чтения карты считыватели Sigur передают в сторону контроллера хэш от считанного PAN-номера, что позволяет избежать компрометации данного номера карты.

Для настройки:

- В программе «Клиент» перейдите в меню «Файл - Настройки». Выберите пункт «Бесконтактная идентификация». Установите сверху пункт «Формат идентификатора пропуска» равным одному из следующих вариантов: Wiegand-26 (3 байта), Wiegand-34 (4 байта) или Wiegand-58 (7 байт). Эта настройка предназначена как для конфигурации выходного формата считывателя, так и для настройки формата получаемых номеров карт с настольного считывателя.
- Перейдите на вкладку «EMV PAN» и установите галочку для опции «Использовать». Тип шифрования на текущий момент не настраивается.
- Рекомендуем отключить использование UID карты в качестве идентификатора пропуска. Для этого перейдите на вкладку «Прочие» и снимите галочку напротив одноимённой опции.
- Если дальнейших настроек считывателя не требуется, то следуйте пунктам раздела «Программирование считывателя мастер-картой» или «Программирование конфигурационным файлом».

## 13. Чтение карт EM Marine и HID® ProxCard II

Считыватели Sigur MR100 Multi поддерживают использование карт EM Marine и HID® ProxCard II® (125 kHz) для идентификации. Для считанных карт всегда возвращается считанный код в формате Wiegand-26. При необходимости можно установить передачу фиксированного facility кода карты или отключить чтение данного типа карт.

Для настройки:

- В программе «Клиент» перейдите в меню «Файл - Настройки».
- Выберите пункт «Mifare и BLE», вкладку «EM Marine» или «HID®».
- Установите галку «Включить чтение карт EM Marine» и/или «Включить чтение карт HID® ProxCard II®» если необходимо читать карты соответствующего формата, либо снимите её, если какой-либо из форматов карт читать не нужно.
- При необходимости можно включить опцию «Использовать фиксированный facility code» и установить необходимое значение (от 0 до 255).
- Если дальнейших настроек считывателя не требуется, то следуйте пунктам раздела «Программирование считывателя мастер-картой» или «Программирование конфигурационным файлом».

## 14. Занесение карт в ПО Sigur



Ниже приведена информация по занесению карт в ПО Sigur. Для добавления карт в другие СКУД обратитесь к их документации.

Занесение карт Mifare и бесконтактных банковских карт в базу ПО Sigur производится с помощью контрольного USB-считывателя ACR 1252U.

Занесение карт EM Marine и HID® ProxCard II® в базу ПО Sigur может быть выполнено как вручную, так и с помощью контрольного USB-считывателя Sigur Reader-EH.

Для добавления карты в базу ПО Sigur через подключенный USB-считыватель:

- В программе «Клиент» перейдите во вкладку «Персонал».
- Выберите нужного сотрудника либо создайте нового кнопкой «Добавить сотрудника в выбранный отдел».
- В том же разделе установите пункт «Действие при чтении карты» равным «Присваивать пропуск текущему объекту» или «Добавлять пропуск текущему объекту».
- Поднесите карту к контрольному считывателю.
- При успешном считывании в поле «Пропуск» появится информация, связанная с данной картой.
- Сохраните внесённые изменения кнопкой «Применить».

## 15. Работа со смартфонами в качестве идентификатора

### 15.1. Идентификация по смартфону, общие сведения

Считыватели Sigur модификации MR100 и MR100 Multi позволяют использовать смартфоны (с установленным приложением «Sigur Доступ») в качестве идентификатора. В случае смартфонов на базе iOS и Android это может быть реализовано с помощью технологии BLE (Bluetooth Low Energy). Также для Android-смартфонов может использоваться альтернативный вариант - технология HCE (Host-based Card Emulation).

BLE-идентификация может происходить в режиме «hands-free» на расстоянии до 10 метров при прямой видимости считывателя. Дальность HCE-идентификации ограничена 9 см.

Трафик между смартфоном и считывателем шифруется AES-алгоритмом шифрования.

Дальность и режим чтения считывателя настраивается конфигурационным файлом или мастер-картой Sigur. Последовательность настройки считывателя подробно описана в разделе [«Программирование считывателя»](#).

Общие требования к смартфонам, а также некоторые комментарии приведены в разделе [«Общие требования к смартфонам и ПО»](#).



Модификации считывателей Sigur MR100 и MR100 Multi также позволяют использовать в качестве идентификатора PAN-номер банковской карты, добавленной в электронный кошелек (МИР Pay, Google Pay, Apple Wallet, Samsung Pay и т.п.). Данный способ не требует установки приложения «Sigur Доступ». Для получения более подробной информации по данному режиму работы обратитесь к разделу [«Работа с банковскими картами»](#).

### 15.2. Настройка системы на работу со смартфонами

Настройка считывателя и ПО на работу со смартфонами производится в несколько этапов:

1. Указание параметров конфигурации работы считывателя в ПО «Клиент» (значение параметров конфигурации описываются в данном пункте).
2. Заполнение реквизитов подключения к серверам исходящей и входящей



- почты.
3. Программирование считывателя мастер-картой или конфигурационным файлом.
  4. Добавление мобильных идентификаторов в ПО.

В программе «Клиент» перейдите в меню «Файл – Настройки – Бесконтактная идентификация». Выберите пункт «Мобильная идентификация» и включите «Использовать».

Здесь нужно настроить следующие поля:

**1. Сервисный пароль** – используется для доступа к считывателю через мобильное приложение «Настройки». Настоятельно не рекомендуется оставлять данное поле в состоянии по умолчанию.

Сервисный пароль считывателя, установленный по умолчанию - «sigur» (без кавычек, с маленькой буквы).

**2. Мобильная идентификация MR** – режим работы считывателя. Доступно три варианта:

- **«Не использовать»** – в данном режиме ни один смартфон с запущенным приложением «Доступ» не будет считан.
- **«Базовый»** – в этом режиме считыватель будет реагировать на любой смартфон, на котором установлено и запущено приложение «Доступ».
- **«Пользовательский»** – в данном режиме работы считыватель будет реагировать только на смартфоны, которым было выслано приглашительное письмо с данного сервера.

**3. Ключ** – используется только в пользовательском режиме работы, и в большинстве случаев достаточно нажать «сгенерировать ключ». Этот ключ не должен меняться в дальнейшем. При его изменении всем сотрудникам потребуется выдать идентификаторы смартфонов повторно.

**4. Расстояние срабатывания BLE** – ориентировочная дальность, на которой будет осуществляться BLE-идентификация. Доступно четыре варианта:

- близкое: - 45 dBm;
- среднее: - 75 dBm;
- далёкое: < - 75 dBm;
- пользовательское (укажите RSSI);

При настройке пользовательской дальности необходимо указать уровень принимаемого сигнала (RSSI) в dBm. Успешная идентификация будет осуществляться при превышении данного уровня. Вы можете выяснить необходимый уровень сигнала для идентификации с помощью мобильного приложения «Настройки».

**5. Политика срабатывания** — правило, при котором будет осуществляться идентификация. Доступно три варианта:

- когда приложение на экране – экран разблокирован и приложение было открыто;
- когда экран разблокирован – экран разблокирован и приложение работает в фоне;
- всегда – приложение запущено в фоне, и идентификация происходит даже при заблокированном экране.

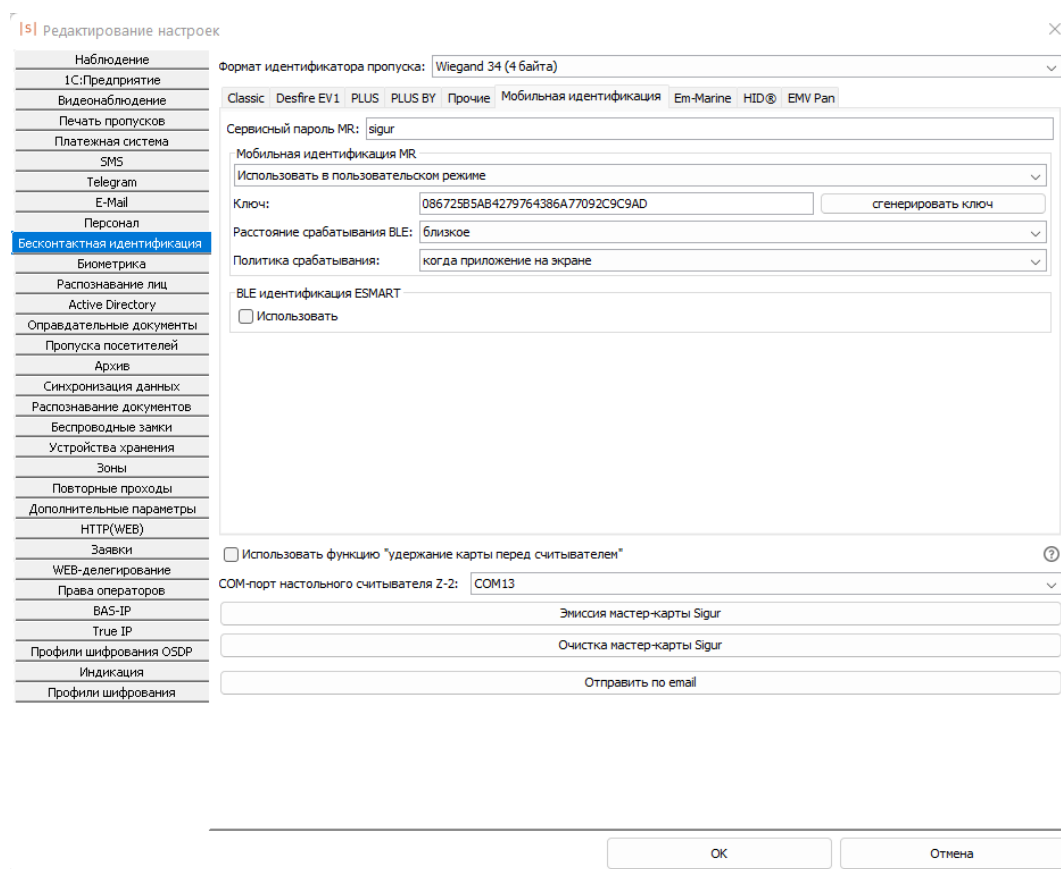


Идентификация при заблокированном экране может повлечь произвольное открытие точек доступа при проходе рядом со считывателями.

Данный режим также понижает общую защищённость системы контроля доступом, т.к. при утере смартфона злоумышленнику не придётся разблокировать экран смартфона, вводя пин-код/графический ключ/производить считывание отпечатка пальца и т.п.

Если дальнейших настроек считывателя не требуется, то следуйте пунктам раздела «Программирование считывателя мастер-картой» или «Программирование конфигурационным файлом».

Если у вас будут несколько считывателей, на которых нужно задать разные дальности срабатывания или политики BLE-идентификации, достаточно будет изменить параметры «Расстояние срабатывания BLE» и «Политика срабатывания», после чего создать ещё одну мастер-карту Sigur или файл конфигурации и загрузить настройки на считыватель. **Изменять поле «Ключ» не нужно!**



Окно настроек мобильной идентификации по смартфону.

### 15.3. Добавление мобильных идентификаторов в ПО



Ниже приведена информация о добавлении идентификаторов смартфонов в ПО Sigur. При использовании считывателя в составе иной СКУД обратитесь к документации данной системы.

Добавление идентификаторов смартфонов происходит путём рассылки пригласительных e-mail уведомлений с сервера СКУД Sigur, в которых будет содержаться специальная ссылка для мобильного приложения «Доступ». При переходе по данной ссылке приложение «Доступ» создаёт ответное письмо, которое должно быть отправлено в ответ.

Пригласительные письма отправляются только в «Пользовательском» режиме работы.

В «Базовом» режиме работы считывателей добавить мобильные идентификаторы можно следующими способами:

- Использовать функцию «Захватывать коды с точки доступа» (см.

- «Руководство пользователя»).
- Вручную, скопировав ID в приложении «Доступ» (нажать кнопку в правом верхнем углу, далее «О программе») и указав его в поле «Пропуск» в программе «Клиент», предварительно укоротив до нужной битности Wiegand.

Выполнение пользователем каких-либо нештатных действий со смартфоном (например, hard reset или переустановка приложения) может повлечь за собой необходимость повторной выдачи мобильного идентификатора. Также известны случаи, когда мобильный идентификатор изменялся при обновлении ОС Android.

### 15.3.1. Отправка приглашительного письма

Для добавления смартфона в систему СКУД Sigur сначала необходимо задать настройки SMTP-сервера для отправки приглашительных e-mail сообщений. Если этого не было сделано ранее, следуйте пунктам раздела «[Настройка доступа к почтовым серверам](#)».

Перейдите во вкладку «Персонал». Выберите нужного сотрудника, либо создайте нового кнопкой «Добавить сотрудника в выбранный отдел». На вкладке «Общее» нажмите «добавить ключ» напротив поля пропуск. Выберите вариант «Выдать мобильный идентификатор»:

Выдача мобильного идентификатора.

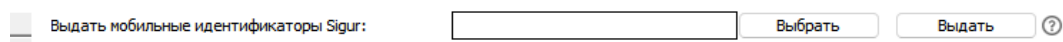
В появившемся поле введите e-mail адрес получателя, либо укажите одну из доступных переменных, в которой хранится адрес электронной почты. Нажмите «ОК» и дождитесь окончания отправки.

Окно ввода Email для отправки приглашительного письма.

Данное письмо будет содержать служебную ссылку для приложения «Доступ», также в нём будут присутствовать ссылки на скачивание данного приложения из Google Play или App Store.

### 15.3.2. Групповая отправка приглачительных писем

При наличии лицензии на программный модуль «Реакция на события» возможно отправить приглачительные письма сразу группе сотрудников. Для этого перейдите в раздел «Файл» - «Настройки» - «Персонал» и в области «Выдать мобильные идентификаторы Sigur» выберите нужных сотрудников.



Окно для отправки группы приглачительных писем.

После выбора нажмите кнопку «Выдать», после чего выбранным сотрудникам будут отправлены приглачительные письма. В качестве email, на которые отправляются письма, система использует значения параметра из учётных карточек сотрудников (на вкладке «Персонал» - подвкладка «Уведомления» выбран «Тип уведомлений» - Email).



Область «Выдать мобильные идентификаторы Sigur» отображается только в том случае, если есть хотя бы один сотрудник, у которого указан Email на вкладке «Персонал» - «Уведомления».

### 15.3.3. Отправка ответного письма

После получения приглачительного письма:



ДОСТУП ПО ТЕЛЕФОНУ

## ДОСТУП ПО ТЕЛЕФОНУ



Здравствуйте!

Вам предоставлен доступ по мобильному идентификатору. Это позволит использовать обычный смартфон как карту доступа. Для начала работы установите приложение «Sigur Доступ»:



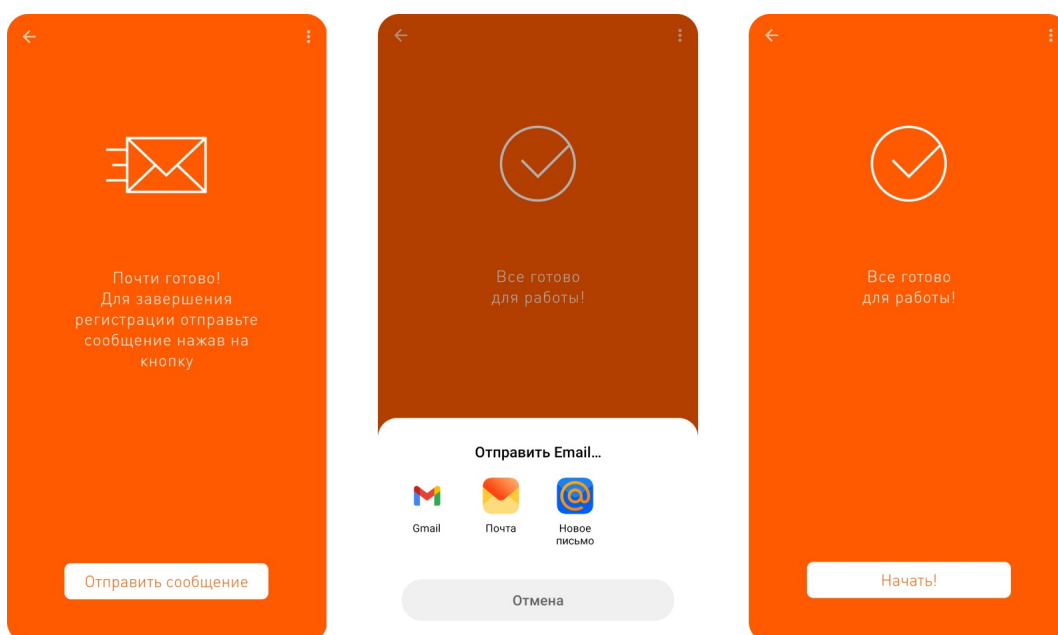
После установки приложения перейдите по [ссылке](#).

Инструкция в приложении поможет настроить устройство. В случае проблем обратитесь к администратору объекта.

Пример приглашительного письма.

- Установите приложение «Sigur Доступ» на смартфон по ссылкам из письма или из [Google Play](#), [App Store](#).
- Перейдите по специальной ссылке из письма, отправленного сервером СКУД Sigur. Вы также можете скопировать ссылку в любой стандартный веб-браузер.
- После перехода по ссылке откроется приложение «Доступ», которое сформирует ответное письмо, содержащее идентификатор, связанный с устройством.
- Данное письмо будет передано в стандартное почтовое приложение устройства, но не будет отправлено. Вам необходимо отправить его вручную.

- Если у вас нет возможности отправить письмо с того же устройства, вы можете скопировать и отправить содержимое письма с любого другого устройства на указанный e-mail адрес. Необязательно отправлять его с того же адреса, на которое пришло приглашительное письмо.
- После отправки ответного письма, в программе «Клиент», у данного сотрудника, автоматически добавится дополнительный идентификатор в поле «Пропуск». Это будет означать успешную привязку идентификатора. С этого момента сотрудник может пользоваться приложением «Доступ».
- Один смартфон может быть зарегистрирован на нескольких серверах СКУД Sigur. Для этого потребуется повторить указанные выше пункты на каждом из объектов.



Отправка ответного письма.

## 15.4. Работа с приложением «Доступ»

Приложение «Доступ» доступно для установки на смартфоны с ОС Android и iOS. В зависимости от ОС смартфона функциональность приложения немного различается. Ключевые отличия: на смартфонах Android доступна идентификация с использованием встроенного NFC-модуля (по технологии HCE) и, в случае использования в ОС «тёмной темы», немного отличается внешний вид приложения. Функция идентификации по BLE доступна и для смартфонов с Android, и для смартфонов с iOS.

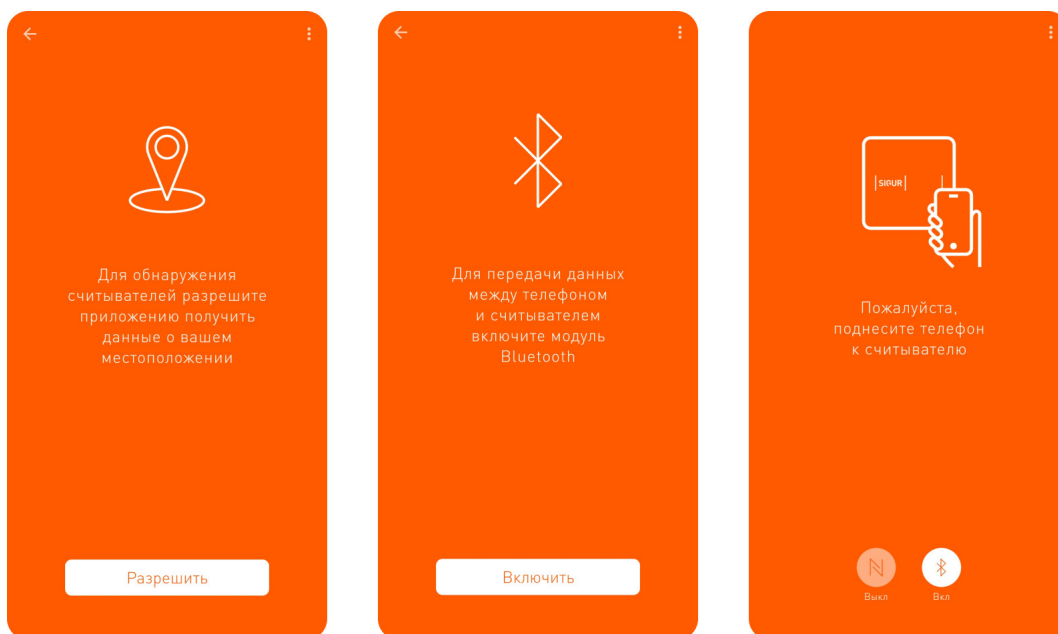
Для идентификации по BLE через приложение «Доступ» включите на смартфоне функцию Bluetooth. В случае некоторых моделей смартфонов на базе Android дополнительно может потребоваться включение функции определения местоположения.

Для идентификации по HCE через приложение «Доступ» включите функцию NFC.



Обратите внимание, что для успешной идентификации по HCE необходимо, чтобы в конфигурации чтения считывателя была отключена функция «Использовать UID карты в качестве идентификатора пропуска» для прочих карт. Данная функция настраивается в ПО «Клиент» при редактировании конфигурации чтения в меню «Файл - Настройки - Бесконтактная идентификация», вкладка «Прочие».

После запуска приложения будут запрошены дополнительные разрешения, предоставьте их приложению. Приложение «Доступ» может работать в фоновом режиме (см. далее таблицу с описанием политик срабатывания считывателя).



Разрешения приложения «Доступ».

В зависимости от установленной политики идентификация требует следующих действий:



**Описание выполнения необходимых условий при действии той или иной политики идентификации.**

<b>Политика срабатывания считывателя</b>	<b>Необходимые условия</b>
Всегда	Смартфону достаточно попасть в область действия считывателя. Идентификация работает даже на заблокированном экране.
Когда экран разблокирован	Смартфон должен находиться в поле действия считывателя, и его экран должен быть разблокирован.
Когда приложение на экране	Смартфон должен находиться в поле действия считывателя, его экран должен быть разблокирован и приложение «Доступ» должно быть запущено на экране смартфона.

На разные считыватели могут быть загружены разные конфигурации настроек: поэтому дальность и политика идентификации могут отличаться.

## 16. Приложение «Sigur Настройки»

### 16.1. Назначение приложения «Sigur Настройки»

Приложение «Sigur Настройки» предназначено для:

- Поиска считывателей в радиусе действия BLE смартфона;
- Обновления внутреннего ПО считывателей;
- Загрузки профиля конфигурации на считыватель;
- Загрузки профиля индикации на считыватель;
- Сброса конфигурации считывателя к заводским настройкам;
- Сброса конфигурации индикации считывателя к заводским параметрам;
- Настройки выходного интерфейса считывателя.

Общие требования к устройствам, а также некоторые комментарии приведены в разделе «Общие требования к смартфонам и ПО».

Скачать данное приложение можно из Google Play: «Sigur Настройки» или по ссылке на нашем сайте.

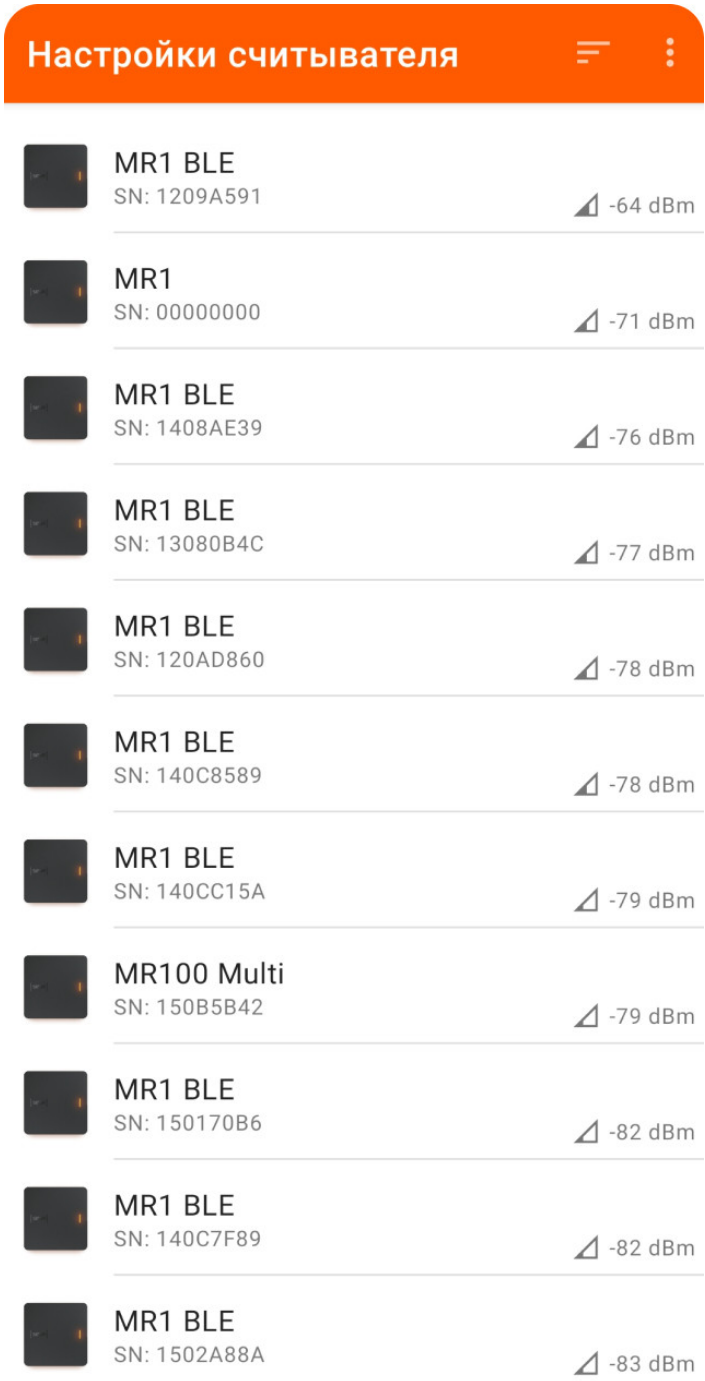
При первом запуске приложения предоставьте ему все запрашиваемые разрешения.

### 16.2. Поиск считывателей в радиусе действия BLE смартфона

Для работы приложения необходимо включить функцию “Bluetooth” на смартфоне. При первом запуске приложения необходимо предоставить все запрашиваемые разрешения.

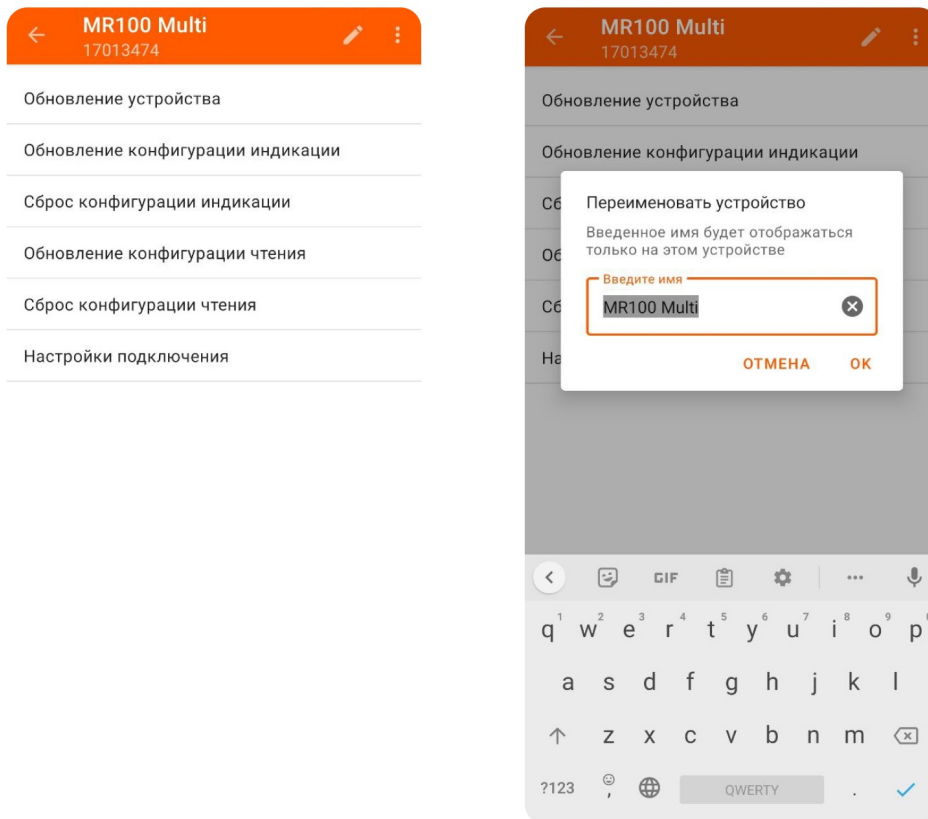
В главном окне “Настройки считывателя” будет отображаться список обнаруженных считывателей. Для каждого считывателя доступна следующая информация:

- название или модель считывателя;
- серийный номер;
- уровень принимаемого сигнала.




Главное окно приложения Sigur "Настройки".


По умолчанию считыватели в списке сортируются по мере обнаружения. При необходимости можно настроить сортировку, нажав на соответствующую кнопку в правом верхнем углу главного окна приложения и выбрав признак сортировки (по мере обнаружения, по силе сигнала или по имени):



Редактирование названия считывателя.

 Введенные наименования сохраняются только на текущем смартфоне.

### 16.3. Обновление внутреннего ПО считывателя

 Данная функция доступна для любой модификации считывателей Sigur. Новые микропрограммы могут исправлять некоторые ошибки предыдущих версий и расширять функции считывателя. Обновление внутреннего ПО считывателя производится с помощью приложения «[Настройки](#)».



Также обновить внутреннее ПО считывателя можно централизованно с рабочего места, но этот способ актуален только для считывателей, подключённых к контроллеру Sigur по интерфейсу OSDP, подробнее процедура описана в соответствующем [разделе](#).

Для проведения операции обновления внутреннего ПО считывателя:

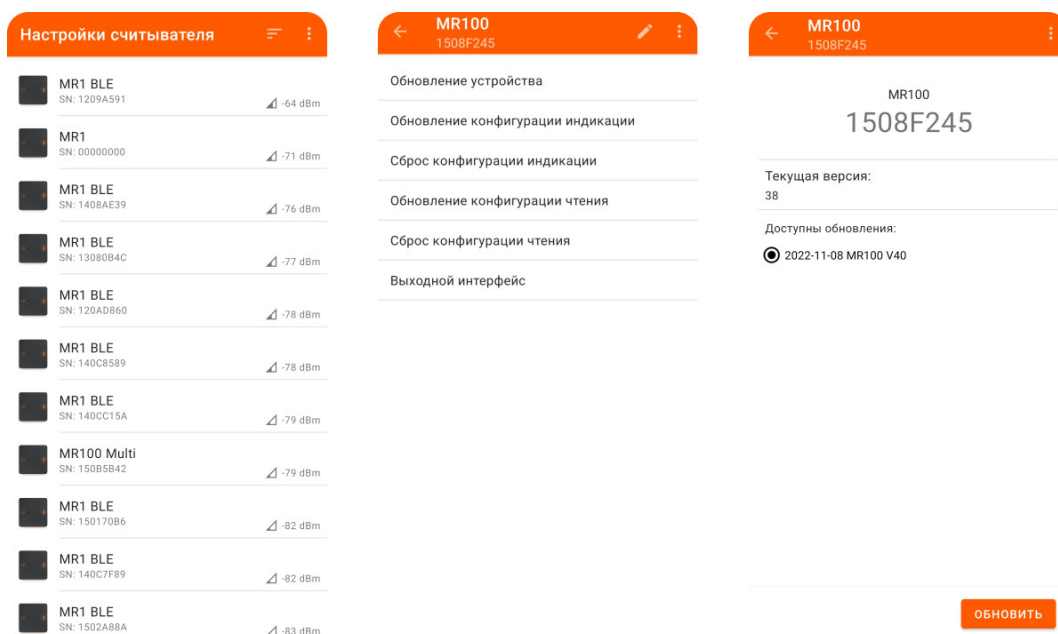
- Включите функции: «Bluetooth», «Определение местоположения» и «Wi-Fi» (или мобильный интернет) на вашем смартфоне и запустите приложение «Настройки». Приложение само будет загружать новые версии микропрограмм считывателя через интернет при первой возможности.
- Подойдите к считывателю(-ям) и откройте приложение «Настройки». Во вкладке «Настройки считывателя» перед вами отобразится список доступных считывателей.
- Выберите из данного списка один из считывателей для обновления микропрограммы, после чего нажмите «Обновление устройства».
- Программа отобразит текущую версию внутреннего ПО считывателя, а также наличие обновления. Выберите одну из доступных микропрограмм и нажмите кнопку «Обновить».
- Введите сервисный пароль устройства. При повторных действиях со считывателем вводить этот пароль не потребуется. Для сброса пароля к стандартному воспользуйтесь функцией сброса параметров считывателя к заводским настройкам. Сервисный пароль считывателя, установленный по умолчанию - «sigur» (без кавычек, с маленькой буквы).
- Дождитесь окончания отправки файла микропрограммы и обновления считывателя. Во время загрузки микропрограммы считыватель изменит свою индикацию: светодиод будет гореть желтым. После успешной загрузки считыватель перейдёт к применению микропрограммы, изменив свою индикацию: светодиод будет моргать желтым и белым цветами.
- Приложение оповестит вас о результате операции, а считыватель издаст характерный звук. После обновления считыватель сразу готов к работе, все прежние настройки сохранятся.

Приложение поддерживает работу сразу с несколькими считывателями.

- Для начала выберите один из считывателей долгим нажатием, после чего можно будет выбрать ещё несколько считывателей короткими нажатиями. Вверху отображается количество выбранных считывателей.
- После завершения выбора нажмите кнопку «Далее» и «Обновление устройства». В данном случае возможны все те же варианты, что и в случае одного считывателя. Если будут какие-то неоднозначности в действиях, приложение отобразит информацию об этом. Вы можете пропустить и не обновлять считыватель нажатием кнопки «Пропуск». Переход к следующему считывателю осуществляется кнопкой

«Следующий».

- После выбора нужных микропрограмм и нажатия кнопки «Обновить» приложение последовательно обновит внутреннее ПО считывателей, прогресс операции вы сможете увидеть в приложении.



Обновление внутреннего ПО считывателя.

## 16.4. Установка специального внутреннего ПО считывателя



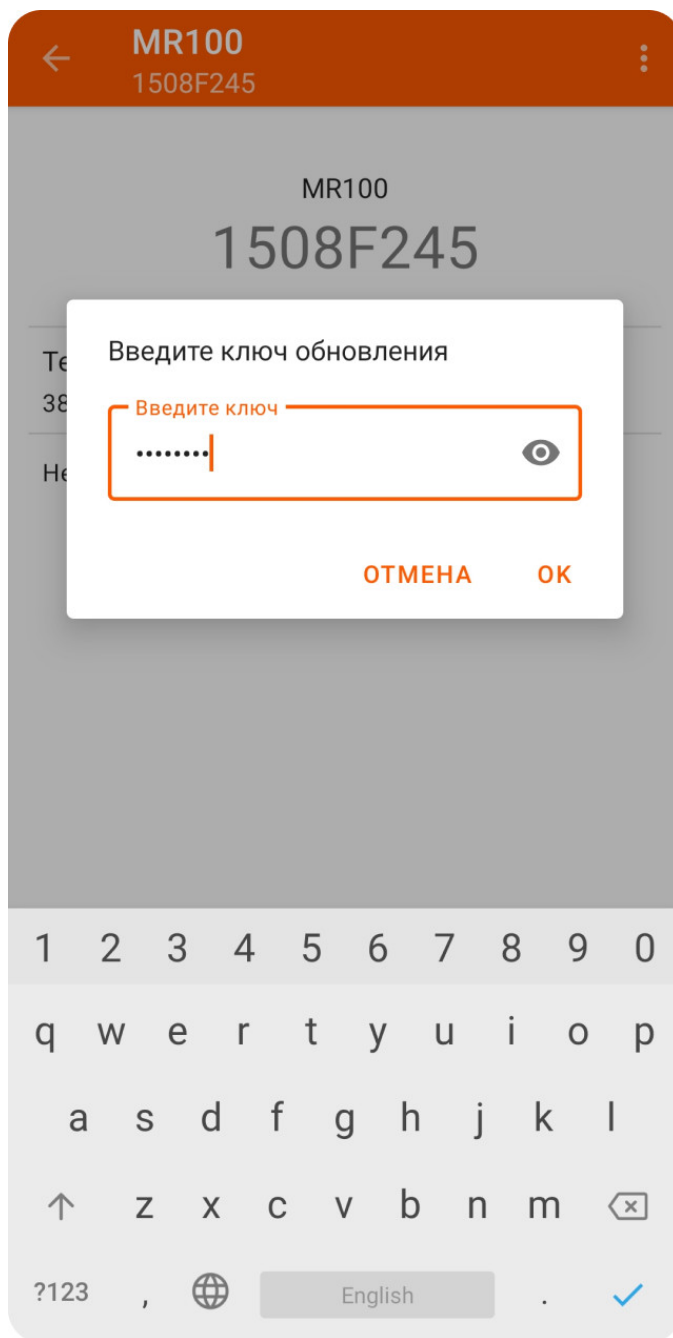
Данная функция доступна для любой модификации считывателей Sigur. Обновление внутреннего ПО считывателя производится с помощью приложения «[Настройки](#)».

Специальное внутреннее ПО считывателя становится доступно при введении лицензионного ключа. Оно позволяет расширять функционал считывателей и решать другие задачи.

Для проведения операции обновления внутреннего ПО считывателя:

- Включите функции: «Bluetooth», «Определение местоположения» и «Wi-Fi» (или мобильный интернет) на вашем смартфоне и запустите приложение «Настройки». Выберите считыватель или несколько считывателей.
- Нажмите кнопку «Обновление устройства».
- В открывшемся окне нажмите на кнопку «Меню» справа сверху.
- Нажмите «Ввести ключ».

- Если у вас есть лицензионный ключ для считывателя, введите его.



Окно ввода ключа специального ПО считывателя.

Приложение попыбует найти микропрограмму считывателя, относящуюся к данному лицензионному ключу. Лицензионный ключ может расширять возможности стандартного ПО считывателей.

Если микропрограмма считывателя будет найдена приложением, то она попадёт в список доступных – вам не придётся вводить лицензионный ключ снова.

После этого обновите выбранные считыватели, нажав кнопку «Обновить».

## 16.5. Загрузка профиля конфигурации чтения на считыватель



Данная функция доступна для любой модификации считывателей Sigur.

Для сброса конфигурации индикации считывателя на смартфоне должно быть установлено приложение «[Настройки](#)».

Для загрузки профиля конфигурации на считыватель:

- Откройте на смартфоне полученное письмо с прикрепленным файлом профиля конфигурации считывателя и нажмите на прикрепленный к письму файл: откроется приложение «Настройки» с уведомлением об успешном добавлении профиля конфигурации. Данный профиль сохранится в приложении, вам не придется нажимать на файл в письме каждый раз.  
Если файл был передан на смартфон иным способом, то достаточно аналогичным образом открыть этот файл с помощью приложения «Настройки».



Также профиль конфигурации можно добавить в приложение вручную. Для этого необходимо включить на смартфоне функции «Bluetooth» и «Определение местоположения», запустить приложение «Настройки», выбрать один из найденных считывателей в списке, после чего из открывшегося списка действий выбрать пункт «Обновление конфигурации чтения». В правом нижнем углу появится кнопка «+», позволяющая вручную выбрать конкретный файл из памяти смартфона.



## НАСТРОЙКА СЧИТЫВАТЕЛЯ SIGUR



Здравствуйте!

Для конфигурации настроек считывателя воспользуйтесь мобильным приложением «Sigur Настройки». Для этого скачайте его из Google Play и установите на свое устройство:



Откройте с помощью приложения подготовленный файл конфигурации, находящийся во вложении к этому письму и передайте его на одно из устройств Sigur по Bluetooth.

Будем рады ответить на вопросы по телефонам и почте:

8 800 620 31 83 (бесплатно по России)  
+7 (495) 665-30-48  
info@sigursys.com

Следите за новостями продуктов и компании во Вконтакте, Facebook или Twitter, а также видеосервисе YouTube.



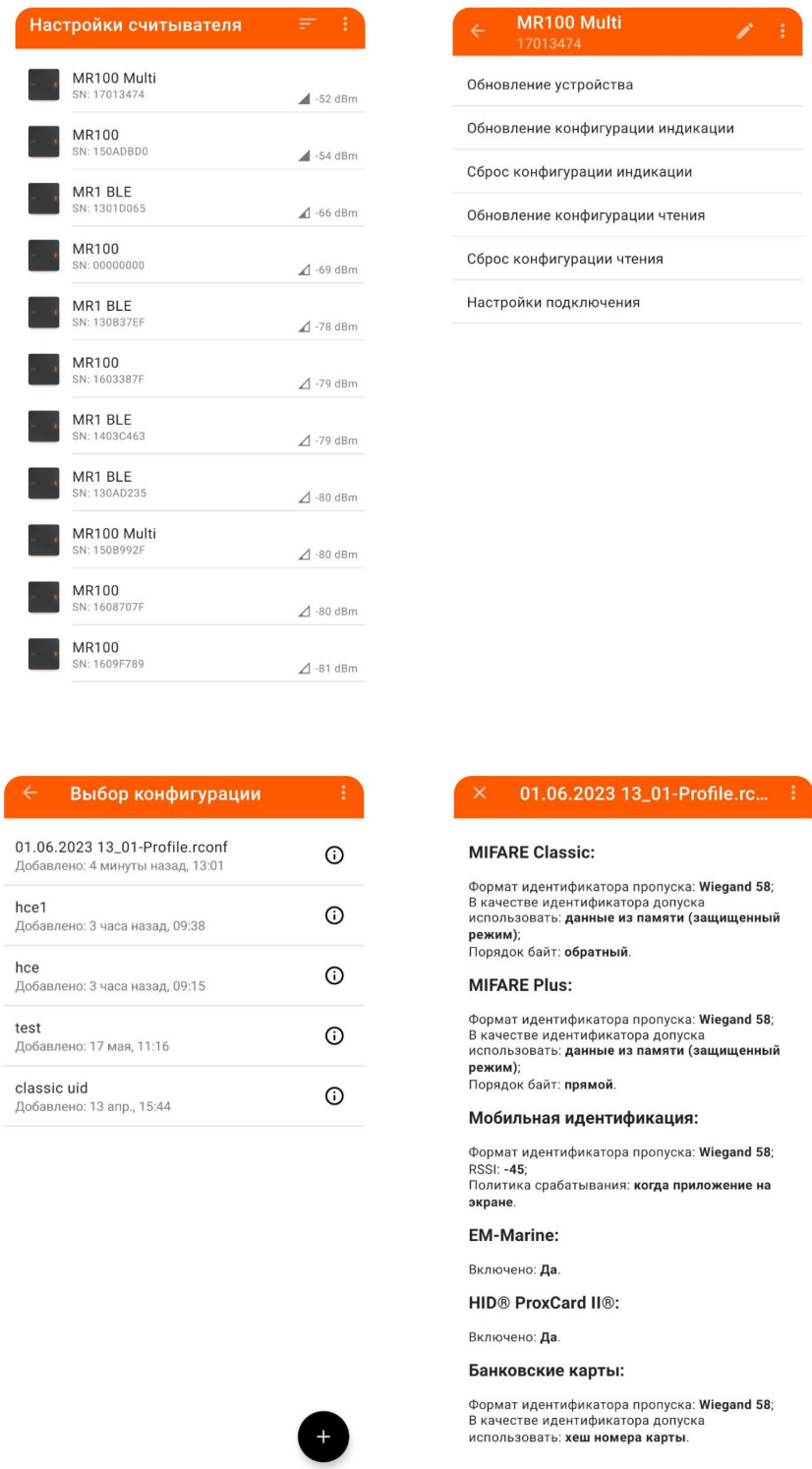
Конфигурация W58



Пример письма, содержащего файл конфигурации считывателя.

- Включите функции: «Bluetooth» и «Определение местоположения» на вашем смартфоне.
- Запустите приложение «Настройки». Выберите считыватель (несколько считывателей), на который необходимо загрузить желаемый профиль конфигурации считывателя.

- Из открывшегося списка действий выберите пункт «Обновление конфигурации чтения».
- Если данный пункт отсутствует в списке действий, то обновите внутреннее ПО считывателя до последней доступной версии.
- Из открывшегося списка профилей конфигурации выберите желаемый и введите сервисный пароль считывателя.
- Дождитесь окончания загрузки конфигурации на считыватель.
- Конфигурация применится по окончании загрузки, перезагрузка считывателя не требуется. После применения новых параметров считыватель издаст характерный звук и приложение уведомит вас об успешности операции.



Пример добавления профиля конфигурации считывателя и просмотр информации о ней.

## 16.6. Сброс конфигурации чтения считывателя



Данная функция доступна для любой модификации считывателей Sigur.

Для проведения операции программного сброса параметров считывателя на смартфоне должно быть установлено приложение «Настройки».

Для проведения операции программного сброса считывателя:

- Включите функции: «Bluetooth» и «Определение местоположения» на вашем смартфоне и запустите приложение «Настройки».
- Выберите считыватель (несколько считывателей), конфигурацию которого необходимо сбросить к заводским параметрам.
- Из открывшегося списка действий выберите пункт «Сброс конфигурации». Если данный пункт отсутствует в списке действий, то обновите внутреннее ПО считывателя до последней доступной версии.
- По окончании процесса сброса конфигурации считыватель издаст характерный звук, а приложение уведомит вас об успешности операции.
- Заводская конфигурация применится по окончании загрузки, перезагрузка считывателя не требуется.

## 16.7. Загрузка профиля индикации на считыватель



Загрузка профиля индикации через мобильное приложение возможна для любой модификации считывателя Sigur MR100 и не зависит от интерфейса, по которому считыватель подключен к контроллеру.

Для загрузки профиля индикации на считыватель на смартфоне должно быть установлено приложение «Настройки». Вы можете установить его по ссылке из письма с прикрепленным профилем индикации (в том случае, если файл с настройками был отправлен на email из ПО Sigur), либо самостоятельно найти его в PlayMarket.

Передать файл на смартфон можно несколькими способами:

- отправить файл на email средствами ПО Sigur.  
Для отправки письма с файлом профиля индикации ПО Sigur потребуется доступ к серверу исходящей почты. Подробная инструкция по настройке реквизитов доступа сервера исходящей почты представлена в разделе «Настройка параметров сервера исходящей почты».

Для отправки файла на email в меню «Файл - Настройки - Индикация» нажмите кнопку «Отправить email» и введите e-mail. На указанный e-mail придёт письмо с прикреплённым файлом конфигурации.



НАСТРОЙКА СЧИТЫВАТЕЛЯ SIGUR

## НАСТРОЙКА СЧИТЫВАТЕЛЯ SIGUR



Здравствуйте!

Для конфигурации индикации считывателя воспользуйтесь мобильным приложением «Sigur Настройки». Для этого скачайте его из Google Play и установите на свое устройство:



Откройте с помощью приложения подготовленный файл конфигурации, находящийся во вложении к этому письму и передайте его на одно из устройств Sigur по Bluetooth.

Будем рады ответить на вопросы по телефонам и почте:

8 800 620 31 83 (бесплатно по России)  
+7 (495) 665-30-48  
info@sigursys.com

Следите за новостями продуктов и компании во Вконтакте, Facebook или Twitter, а также видеосервисе YouTube.

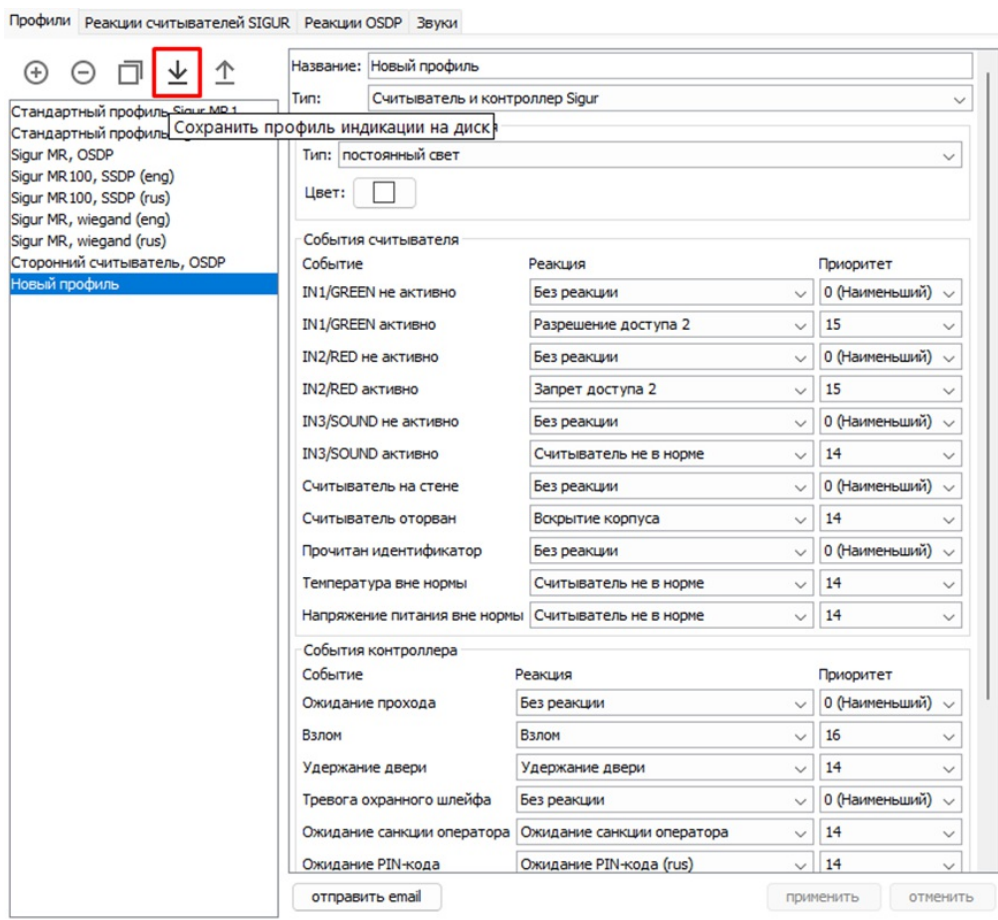


Профиль индикации



Пример письма, содержащего профиль индикации.

- можно сохранить файл на компьютер, а затем передать на смартфон альтернативными способами (отправить через мессенджер/использовать внешний накопитель и пр.). Для того, чтобы сохранить файл на диск необходимо в меню Файл - Настройки - Индикация - Профили выбрать нужный профиль и нажать на соответствующую кнопку. После чего система предложит ввести произвольное название файла профиля индикации и выбрать каталог для сохранения.

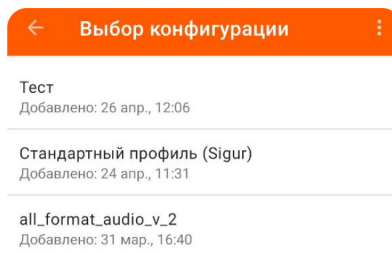


Сохранение файла профиля индикации на диск.

Для загрузки профиля индикации на считыватель:

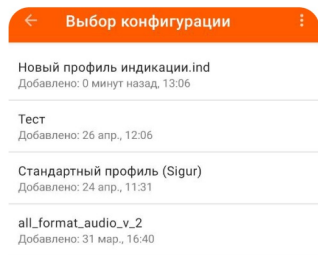
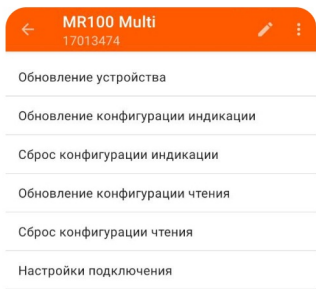
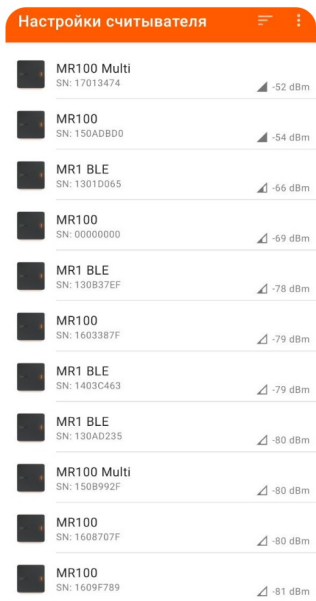
1. Откройте на смартфоне полученный файл профиля индикации с помощью приложения «Настройки». После этого автоматически запустится приложение «Настройки» с уведомлением об успешном добавлении профиля индикации. Данный профиль сохранится в приложении, вам не придётся открывать файл каждый раз.

Либо файл можно загрузить в приложение вручную. Для этого необходимо включить функции «Bluetooth» и «Определение местоположения», запустить приложение «Настройки», в главном окне выбрать произвольный считыватель, в меню действий нажать на «Обновление конфигурации индикации», после чего откроется хранилище конфигураций. В правом нижнем углу можно нажать на кнопку «+» и добавить профиль индикации, выбрав файл из памяти смартфона.



Хранилище конфигураций индикации в приложении «Настройки».

2. Включите функции: «Bluetooth» и «Определение местоположения» на вашем смартфоне.
3. Запустите приложение «Настройки». Выберите считыватель или несколько считывателей, на который необходимо загрузить желаемый профиль индикации.
4. Из открывшегося списка действий выберите пункт «Обновление конфигурации индикации».
5. Если данный пункт отсутствует в списке действий, то убедитесь в том, что модель считывателя соответствует требованиям выше и обновите внутреннее ПО считывателя до последней доступной версии.
6. Из открывшегося списка профилей индикации выберите желаемый и введите сервисный пароль считывателя.
7. Дождитесь окончания загрузки конфигурации на считыватель. Конфигурация индикации применится по окончании загрузки, перезагрузка считывателя не требуется.



Добавление нового профиля индикации.



## 16.8. Сброс конфигурации индикации считывателя



Данная функция доступна для любой модификации считывателя Sigur MR100.

Для сброса конфигурации индикации считывателя на смартфоне должно быть установлено приложение «[Настройки](#)».

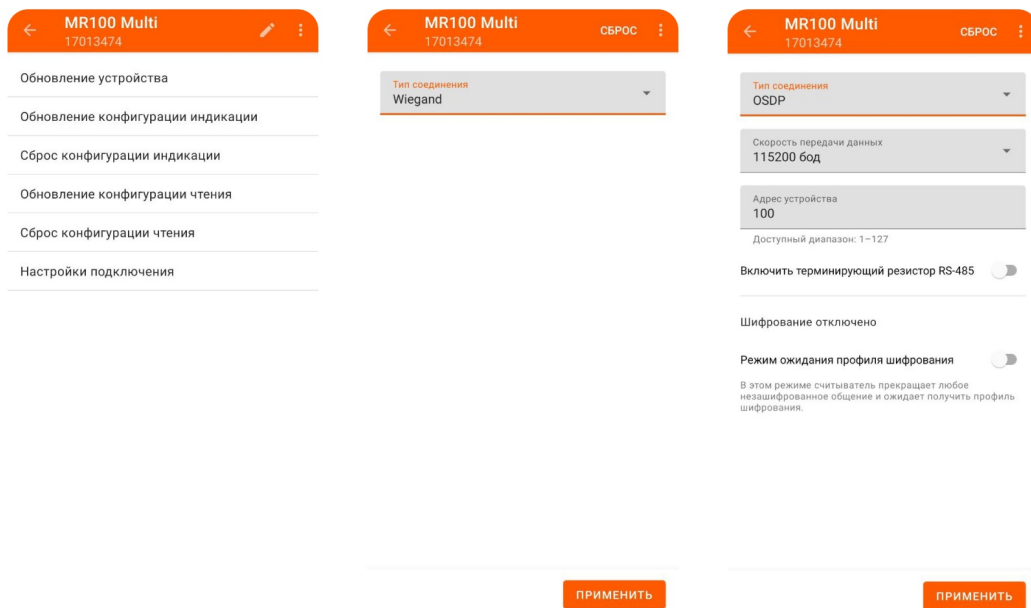
Для сброса индикации считывателя к заводским настройкам:

- Откройте приложение «Настройки» и выберите считыватель из списка.
- Из открывшегося списка действий выберите пункт «Сброс конфигурации индикации».
- Подтвердите операцию и введите сервисный пароль считывателя.
- Дождитесь окончания загрузки конфигурации на считыватель. Конфигурация индикации применится по окончании загрузки, перезагрузка считывателя не требуется.

## 16.9. Настройка выходного интерфейса считывателя

Для установки выходного интерфейса считывателя:

- Откройте приложение «Настройки» и выберите считыватель из списка.
- Из открывшегося списка действий выберите пункт «Выходной интерфейс».
- Выберите нужный режим работы - Wiegand или OSDP. Если считыватель подключается к контроллеру по OSDP, необходимо также настроить для него:
  - Скорость передачи данных - скорость обмена на RS485-шлейфе между контроллером и подключенными к нему считывателями. Возможные скорости: 9600, 19200, 38400, 57600, 115200 бод.
  - Адрес устройства - уникальный адрес считывателя на RS485-шлейфе. Целое число от 1 до 127.
  - Включение терминирующего резистора RS485 - требуется установить, если устройство является первым или последним на шлейфе.
  - Установочный режим шифрования - требуется установить, если считыватель необходимо перевести в режим шифрования данных, передаваемых по OSDP, и загрузить профиль шифрования.
- Подтвердите операцию и при необходимости введите сервисный пароль считывателя.
- Дождитесь окончания загрузки настроек на считыватель. Настройки применятся по окончании загрузки, перезагрузка считывателя не требуется.



Установка выходного интерфейса считывателя.

## 17. Шифрование данных, передаваемых по OSDP

При работе считывателей по интерфейсу OSDP в целях повышения уровня безопасности опционально может быть включено шифрование передаваемых данных между считывателем и контроллером.



Для использования функционала шифрования данных считыватель может быть подключён по интерфейсу OSDP как к контроллеру Sigur, так и к контроллеру стороннего производителя.

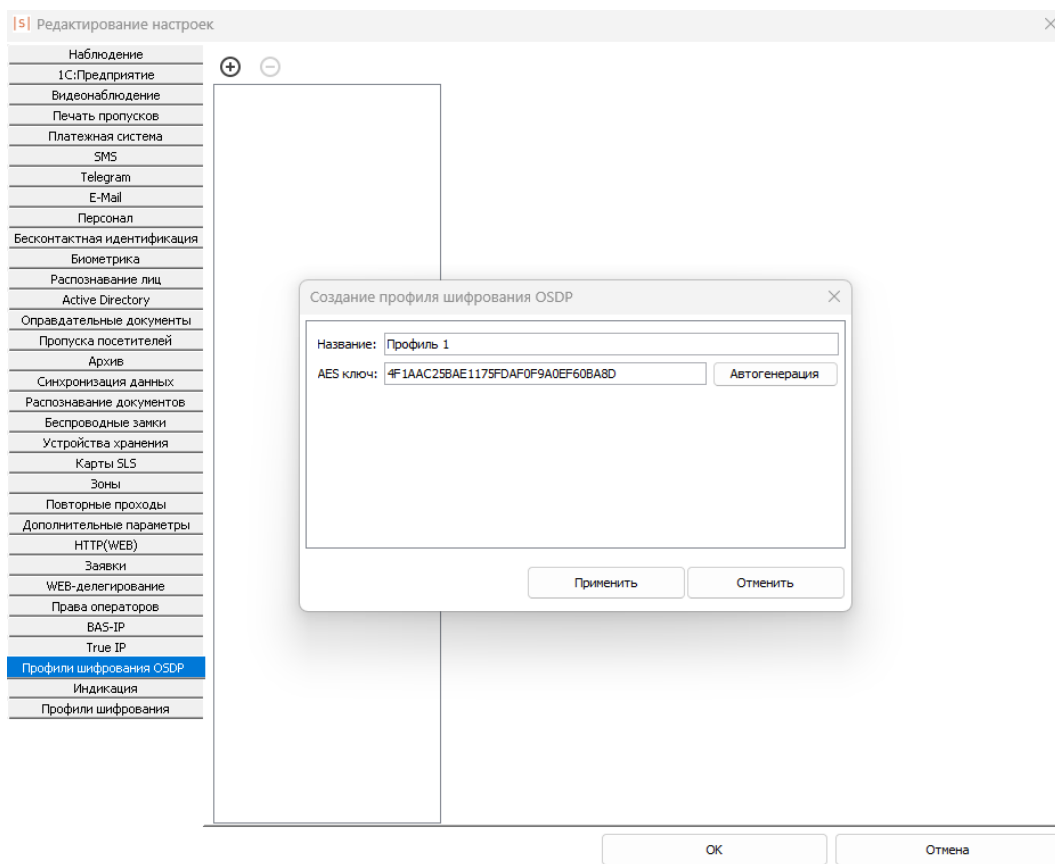
Настройка такого режима работы состоит из следующих этапов:

- [Создание профиля шифрования](#)
- [Применение профиля шифрования](#)

### 17.1. Создание профиля шифрования OSDP

Создание и управление профилями шифрования осуществляется в программе «Клиент».

Чтобы создать новый профиль шифрования OSDP, необходимо перейти в меню «Файл - Настройки - Профили шифрования OSDP». В открывшемся окне нажать на кнопку , задать название профиля шифрования и заполнить самостоятельно или сгенерировать автоматически AES ключ с помощью кнопки «Автогенерация».



Окно редактирования настроек профилей шифрования OSDP..

Когда все данные введены необходимо нажать на кнопку «Применить» и созданный профиль шифрования отобразится в списке.

## 17.2. Применение профиля шифрования OSDP

Для того, что применить профиль шифрования необходимо последовательно выполнить следующие действия:

1. Убедиться, что между считывателем и контроллером установлена связь. Если считыватель подключен к контроллеру Sigur, то для этого в программе «Клиент» на вкладке «Оборудование» нужно выделить точку доступа контроллера, нажать кнопку «Настройки». На вкладке «OSDP устройства» считыватель должен быть назначен на конкретный порт контроллера, для которого в качестве статуса отображается сообщение «Есть связь».

Редактирование настроек

Конфигурация: (Пользовательская)

Общее | Точка доступа 1 | Точка доступа 2 | Точка доступа 3 | Точка доступа 4 | OSDP устройства

Скорость передачи данных контроллера (все порты): 115200 бод

Настройки портов

Задействовать для OSDP	Адрес	Статус	Загрузить профиль индикации	Профиль шифрования	Контрольная сумма	Загрузить прошивку на считыватель	Конфигурация чтения
<input checked="" type="checkbox"/>	100	Есть связь	Сменить профиль индикации	(нет)	CRC16	Выбрать	Загрузить
<input type="checkbox"/>	3	Нет связи	Сменить профиль индикации	(нет)	CRC16	Выбрать	Загрузить
<input type="checkbox"/>	0	Нет связи	Сменить профиль индикации	(нет)	CRC16	Выбрать	Загрузить
<input type="checkbox"/>	0	Нет связи	Сменить профиль индикации	(нет)	CRC16	Выбрать	Загрузить

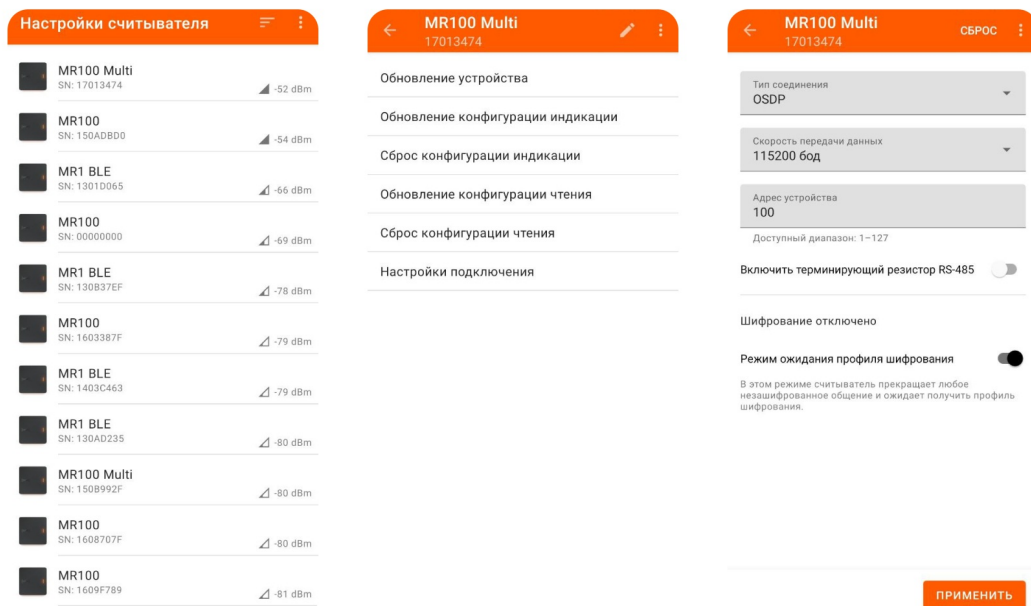
Применить

Отображать только базовые настройки

OK Отмена

Проверка состояния связи по OSDP между считывателем и контроллером через ПО «Клиент».

2. В мобильном приложении Sigur «Настройки» выбрать интересующий считыватель и в списке действий для него перейти в «Настройки подключения», активировать опцию «Режим ожидания профиля шифрования» и нажать кнопку «Применить», чтобы внесённые изменения применились на считыватель.



Активация режима ожидания профиля шифрования на считывателе.

3. Загрузить профиль шифрования с контроллера на считыватель. Если считыватель подключен к контроллеру Sigur, то в программе «Клиент» в меню настроек точки доступа на вкладке «OSDP устройства» для конкретного порта контроллера назначить ранее созданный профиль шифрования, нажать кнопку «Применить».

Общее Точка доступа 1 Точка доступа 2 Точка доступа 3 Точка доступа 4 OSDP устройства

Скорость передачи данных контроллера (все порты): 115200 бод

Настройки портов

Закрепить для OSDP	Адрес	Статус	Загрузить профиль индикации	Профиль шифрования	Контрольная сумма	Загрузить прошивку на считыватель	Конфигурация чтения
<input checked="" type="checkbox"/>	100	Ошибка	Сменить профиль индикации	Профиль 1	CRC16	Выбрать	Загрузить
<input type="checkbox"/>	3	Нет связи	Сменить профиль индикации	(нет)	CRC16	Выбрать	Загрузить
<input type="checkbox"/>	0	Нет связи	Сменить профиль индикации	(нет)	CRC16	Выбрать	Загрузить
<input type="checkbox"/>	0	Нет связи	Сменить профиль индикации	(нет)	CRC16	Выбрать	Загрузить

Применить

Отображать только базовые настройки

OK Отмена

Назначение профиля шифрования OSDP.

4. Далее необходимо убедиться, что статус связи после применения профиля шифрования OSDP отображается как «Есть связь».

Общее Точка доступа 1 Точка доступа 2 Точка доступа 3 Точка доступа 4 OSDP устройства

Скорость передачи данных контроллера (все порты): 115200 бод

Настройки портов

Закрепить для OSDP	Адрес	Статус	Загрузить профиль индикации	Профиль шифрования	Контрольная сумма	Загрузить прошивку на считыватель	Конфигурация чтения
<input checked="" type="checkbox"/>	100	Есть связь	Сменить профиль индикации	Профиль 1	CRC16	Выбрать	Загрузить
<input type="checkbox"/>	3	Нет связи	Сменить профиль индикации	(нет)	CRC16	Выбрать	Загрузить
<input type="checkbox"/>	0	Нет связи	Сменить профиль индикации	(нет)	CRC16	Выбрать	Загрузить
<input type="checkbox"/>	0	Нет связи	Сменить профиль индикации	(нет)	CRC16	Выбрать	Загрузить

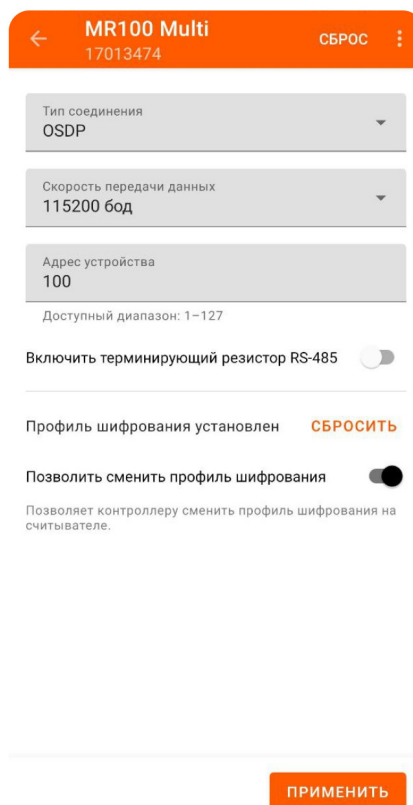
Применить

Отображать только базовые настройки

OK Отмена

Проверка состояния связи по OSDP между считывателем и контроллером после применения профиля шифрования OSDP.

В мобильном приложении также можно увидеть, что профиль шифрования успешно установлен.



Меню настроек подключения считывателя при установленном профиле шифрования.

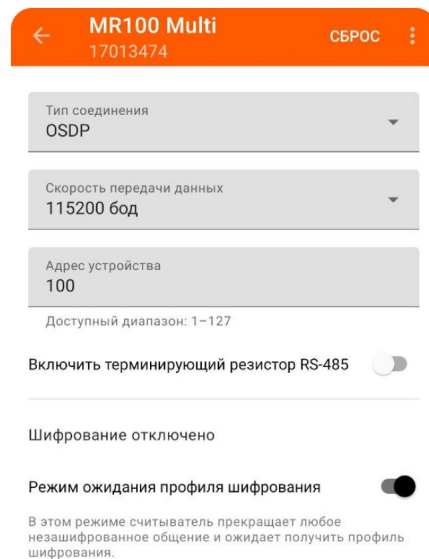
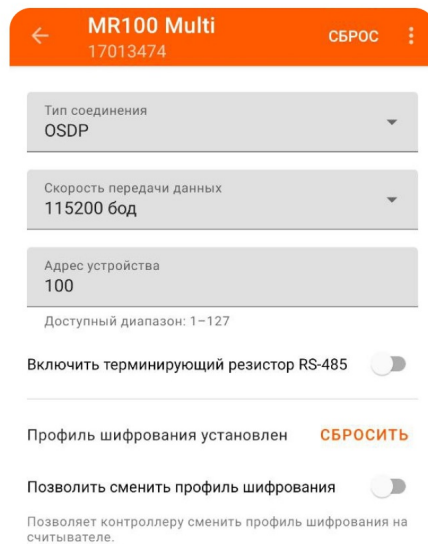
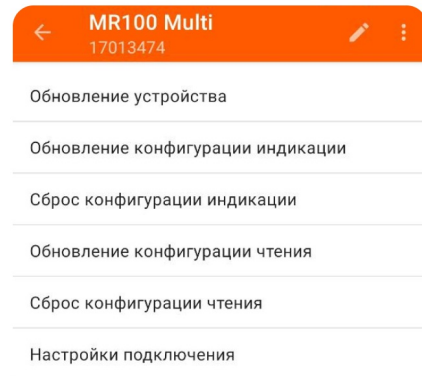
### 17.3. Сброс профиля шифрования

При необходимости профиль шифрования OSDP можно сбросить. Сброс профиля шифрования OSDP необходим в случае, если по каким-то причинам (удалена база данных, сервер вышел из строя, человеческий фактор) была удалён профиль шифрования OSDP в программе «Клиент», а восстановить значение AES-ключа не представляется возможным.

Чтобы сбросить профиль шифрования необходимо выполнить следующие действия:

1. В мобильном приложении Sigur «Настройки» выбрать интересующий считыватель и в списке действий для него перейти в «Настройки подключения».
2. Нажать на кнопку «Сбросить» напротив пункта «Профиль шифрования установлен» и нажать кнопку «Применить», чтобы внесённые изменения применились на считыватель.





Процедура сброса профиля шифрования OSDP на считывателе.

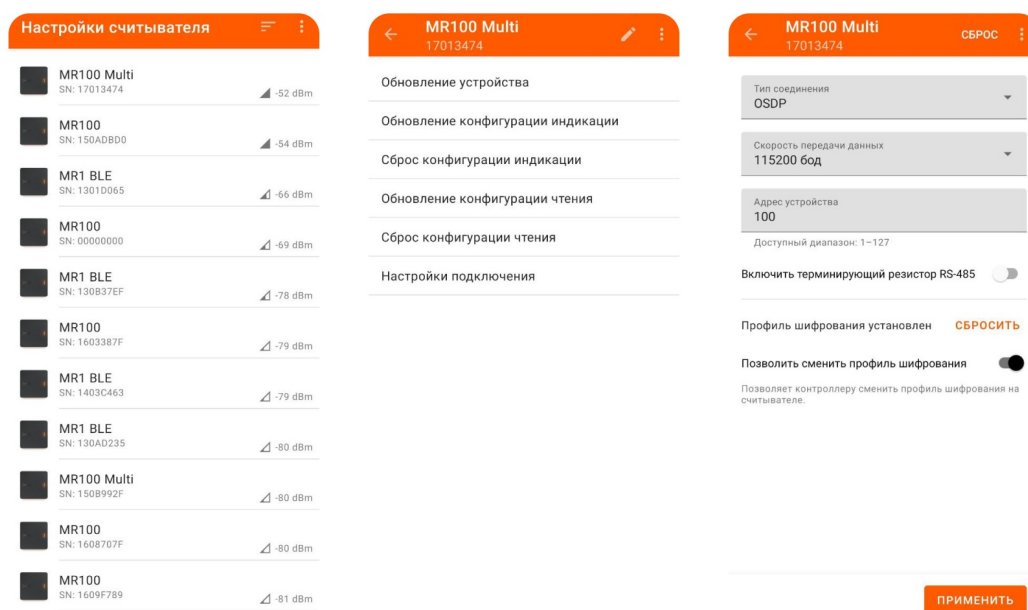
## 17.4. Изменение профиля шифрования

Если на считывателе уже установлен профиль шифрования, то опционально на считывателе можно активировать функцию, позволяющую изменить текущий профиль на другой с помощью команды протокола OSDP со стандартным AES-ключом.

В частности, если контроллеру не будет известен ранее установленный на считывателе профиль шифрования OSDP с определенным AES-ключом, то он сможет установить на считыватель новый профиль шифрования (с новым AES-ключом), и этот профиль будет передан на считыватель с помощью команды OSDP-протокола со стандартным AES-ключом.

Для активации опции «Позволить сменить профиль шифрования» необходимо выполнить следующие действия:

- В мобильном приложении Sigur «Настройки» выбрать интересующий считыватель и в списке действий для него перейти в «Настройки подключения»;
- Активировать опцию «Позволить сменить профиль шифрования» и нажать кнопку «Применить», чтобы внесённые изменения применились на считыватель.
- Если считыватель подключён к контроллеру Sigur, то далее можно выбрать новый профиль шифрования в настройках точки доступа в программе «Клиент».



Процесс активации опции «Позволить сменить профиль шифрования».

Если же данная опция не будет активирована, то считыватель будет игнорировать попытки изменения текущего профиля шифрования с помощью команд со стандартным AES-ключом, полученных по OSDP. В таком случае профиль шифрования можно будет изменить только при условии, что между контроллером и считывателем уже установлено зашифрованное соединение или после сброса профиля шифрования на считывателе.

## 18. Обновление внутреннего ПО считывателя через программу «Клиент»

Новые микропрограммы могут исправлять некоторые ошибки предыдущих версий и расширять функции считывателя.



Этот способ актуален только для тех случаев, когда считыватель подключён к контроллеру Sigur по интерфейсу OSDP, иными словами данная возможность - отличительная особенность протокола SSDP, позволяющая централизованно с рабочего места обновить микропрограмму считывателя до актуальной версии.

Если используется иная конфигурация системы, воспользуйтесь альтернативным способом - обновите микропрограмму считывателя с помощью мобильного приложения. Процедура подробно описана в соответствующем [разделе](#).

Для обновления микропрограммы считывателя через ПО «Клиент» должны выполняться следующие технические требования:

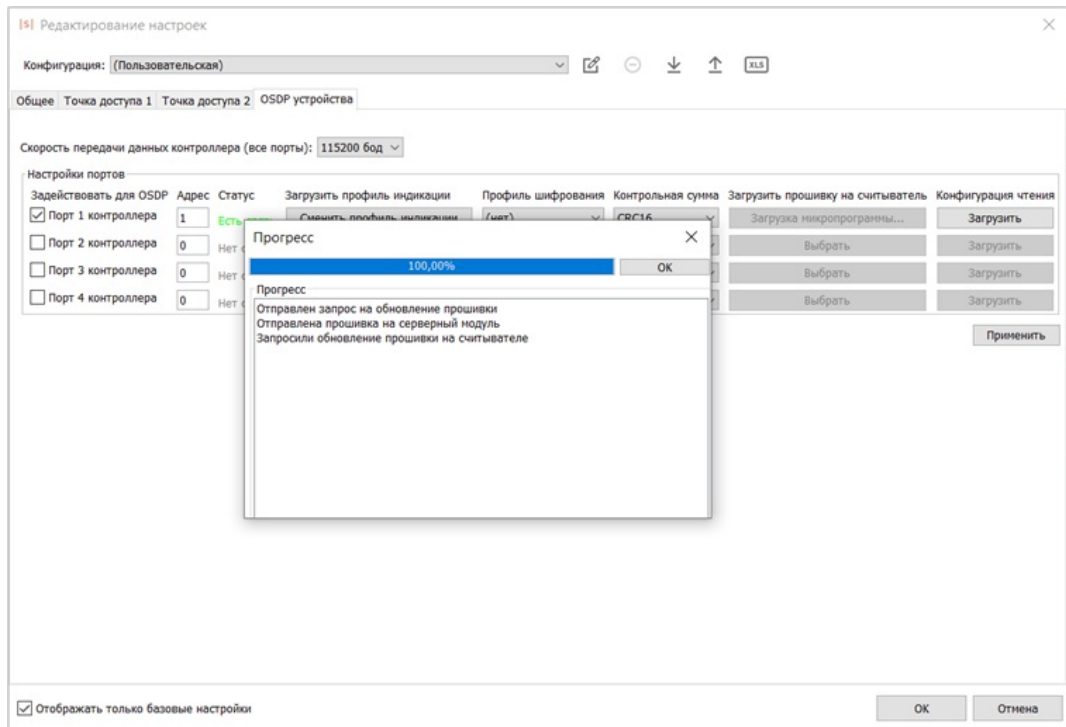
- версия микропрограммы считывателя должна быть не ниже 43;
- версия микропрограммы контроллера должна быть не ниже 18;
- версия ПО должна быть не ниже 1.1.1.48 (подойдёт [бесплатная версия](#)).



Для процедуры необходим файл актуальной версии микропрограммы считывателя. Запросить файл можно, обратившись в [техническую поддержку Sigur](#).

Для проведения операции обновления микропрограммы считывателя необходимо выполнить следующие действия:

- В программе «Клиент» в меню настроек точки доступа на вкладке «OSDP устройства» для конкретного порта контроллера нажать кнопку «Выбрать» в блоке «Загрузить прошивку на считыватель». Откроется окно с выбором файла микропрограммы считывателя. Необходимо выбрать файл и нажать на кнопку «ОК». Начнётся процесс загрузки микропрограммы на считыватель. Во время загрузки кнопка «Выбрать» будет изменена на «Загрузка микропрограммы» и будет неактивна, а в журнале системных событий появится событие «Начало применения микропрограммы на считыватель»;



Процесс загрузки микропрограммы на считыватель через программу «Клиент».

- При успешном окончании загрузки кнопка «Выбрать» примет свое стандартное состояние, а в журнале системных событий (подробнее можно ознакомиться в разделе «[Журнал системных событий](#)») появится событие «Микропрограмма считывателя успешно обновлена».

## 19. Журнал системных событий

Для отслеживания процесса выполнения процедур обновления профиля индикации, профиля чтения карт и микропрограммы считывателя через протокол SSDP в программе «Клиент» предусмотрен «Журнал системных событий».

События в журнале можно просмотреть, нажав на кнопку «Показать журнал системных событий», расположенную на вкладке «Оборудование»:



Данная кнопка появляется автоматически, если есть как минимум одно событие.

В журнале указана следующая информация:

- Дата и время события;
- Параметры. Содержит такую информацию как:
  - серийный номер контроллера;
  - порт, на который подключён считыватель, с которым связано данное событие;
  - название профиля индикации (опционально).
- Тип события.

Журнал системных событий		
Дата и время	Параметры	Событие
2023-05-22 08:4...	Серийный номер контроллера: 1701482E, порт: 1, профиль индикации: "Sigur MR100, SSDP ...	Начало загрузки профиля индикации на считыватель.
2023-05-22 08:5...	Серийный номер контроллера: 1701482E, порт: 1, профиль индикации: "Sigur MR100, SSDP ...	Профиль индикации успешно загружен на считыватель.
2023-05-22 10:2...	Серийный номер контроллера: 1701482E, порт: 1, профиль индикации: "Sigur MR100, SSDP ...	Начало загрузки профиля индикации на считыватель.
2023-05-22 10:2...	Серийный номер контроллера: 1701482E, порт: 1, профиль индикации: "Sigur MR100, SSDP ...	Профиль индикации успешно загружен на считыватель.
2023-05-22 10:3...	Серийный номер контроллера: 1701482E, порт: 1, профиль индикации: "Sigur MR100, SSDP ...	Начало загрузки профиля индикации на считыватель.
2023-05-22 10:3...	Серийный номер контроллера: 1701482E, порт: 1, профиль индикации: "Sigur MR100, SSDP ...	Профиль индикации успешно загружен на считыватель.
2023-05-22 10:3...	Серийный номер контроллера: 1701482E, порт: 1, профиль индикации: "Sigur MR100, SSDP ...	Начало загрузки профиля индикации на считыватель.
2023-05-22 10:3...	Серийный номер контроллера: 1701482E, порт: 1, профиль индикации: "Sigur MR100, SSDP ...	Профиль индикации успешно загружен на считыватель.
2023-05-22 10:3...	Серийный номер контроллера: 1701482E, порт: 1, профиль индикации: "Sigur MR100, SSDP ...	Начало загрузки профиля индикации на считыватель.
2023-05-22 10:3...	Серийный номер контроллера: 1701482E, порт: 1, профиль индикации: "Sigur MR100, SSDP ...	Профиль индикации успешно загружен на считыватель.
2023-05-22 10:5...	Серийный номер контроллера: 1701482E, порт: 1, профиль индикации: "Sigur MR100, SSDP ...	Начало загрузки профиля индикации на считыватель.
2023-05-22 10:5...	Серийный номер контроллера: 1701482E, порт: 1, профиль индикации: "Sigur MR100, SSDP ...	Профиль индикации успешно загружен на считыватель.
2023-05-22 14:1...	Серийный номер контроллера: 1701482E, порт: 1.	Запуск процесса обновления профиля чтения карт считывателя.
2023-05-22 14:1...	Серийный номер контроллера: 1701482E, порт: 1.	Начало применения профиля чтения карт на считыватель.
2023-05-22 14:1...	Серийный номер контроллера: 1701482E, порт: 1.	Профиль чтения карт считывателя успешно обновлен.

Отфильтровать отображаемые события

Отображение событий в журнале системных событий.

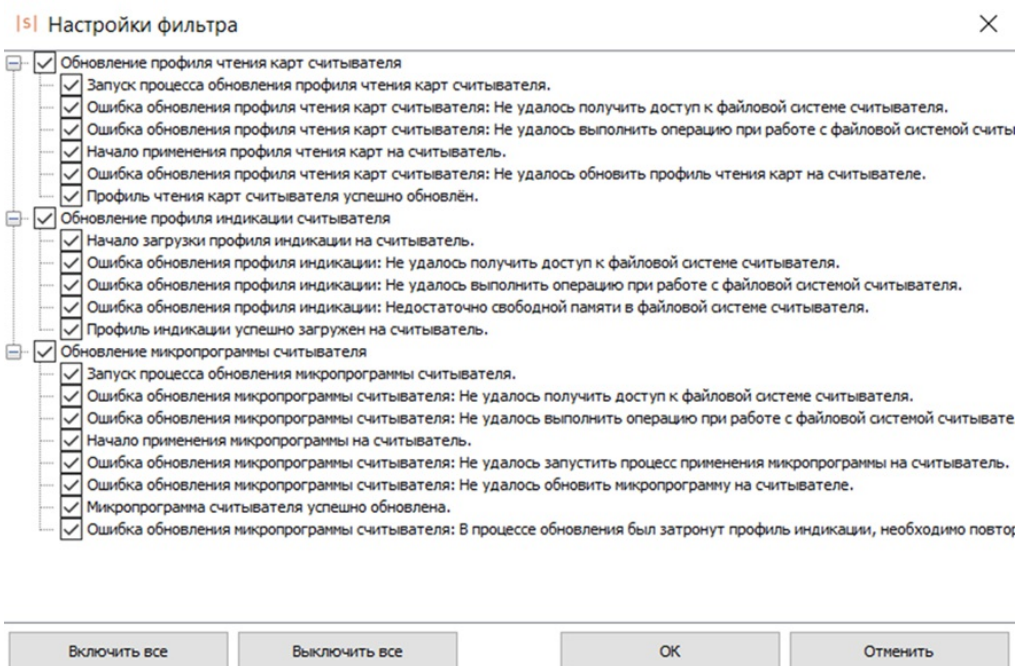
В журнале отображаются такие события как:

- События, связанные с обновлением профиля чтения карт считывателя:
  - Запуск процесса обновления профиля чтения карт считывателя.
  - Ошибка обновления профиля чтения карт считывателя: Не удалось получить доступ к файловой системе считывателя.
  - Ошибка обновления профиля чтения карт считывателя: Не удалось выполнить операцию при работе с файловой системой считывателя.
  - Начало применения профиля чтения карт на считыватель.
  - Ошибка обновления профиля чтения карт считывателя: Не удалось обновить профиль чтения карт на считывателе.
  - Профиль чтения карт считывателя успешно обновлён.
- События, связанные с профилем индикации считывателя:
  - Начало загрузки профиля индикации на считыватель.
  - Ошибка обновления профиля индикации: Не удалось получить доступ к файловой системе считывателя.
  - Ошибка обновления профиля индикации: Не удалось выполнить операцию при работе с файловой системой считывателя.
  - Ошибка обновления профиля индикации: Недостаточно свободной памяти в файловой системе считывателя.
  - Профиль индикации успешно загружен на считыватель.
- События, связанные с обновлением микропрограммы считывателя:

- Запуск процесса обновления микропрограммы считывателя.
- Ошибка обновления микропрограммы считывателя: Не удалось получить доступ к файловой системе считывателя.
- Ошибка обновления микропрограммы считывателя: Не удалось выполнить операцию при работе с файловой системой считывателя.
- Начало применения микропрограммы на считыватель.
- Ошибка обновления микропрограммы считывателя: Не удалось запустить процесс применения микропрограммы на считыватель.
- Ошибка обновления микропрограммы считывателя: Не удалось обновить микропрограмму на считывателе.
- Микропрограмма считывателя успешно обновлена.
- Ошибка обновления микропрограммы считывателя: В процессе обновления был затронут профиль индикации, необходимо повторно загрузить его на считыватель.

Для поиска нужных событий используются фильтры. Доступны следующие фильтры:

- «Тип события». Фильтрация отображаемых событий по типу. Данный фильтр можно настроить, нажав на кнопку «Выбор типа события».



Настройки фильтра по типу события.

- «По дате и времени». С помощью данного фильтра можно отобразить события за нужный период, указав необходимые даты и время в соответствующих полях.

От: 10.05.2023 00:00 До: 22.05.2023 23:59

Настройки фильтра по дате и времени.

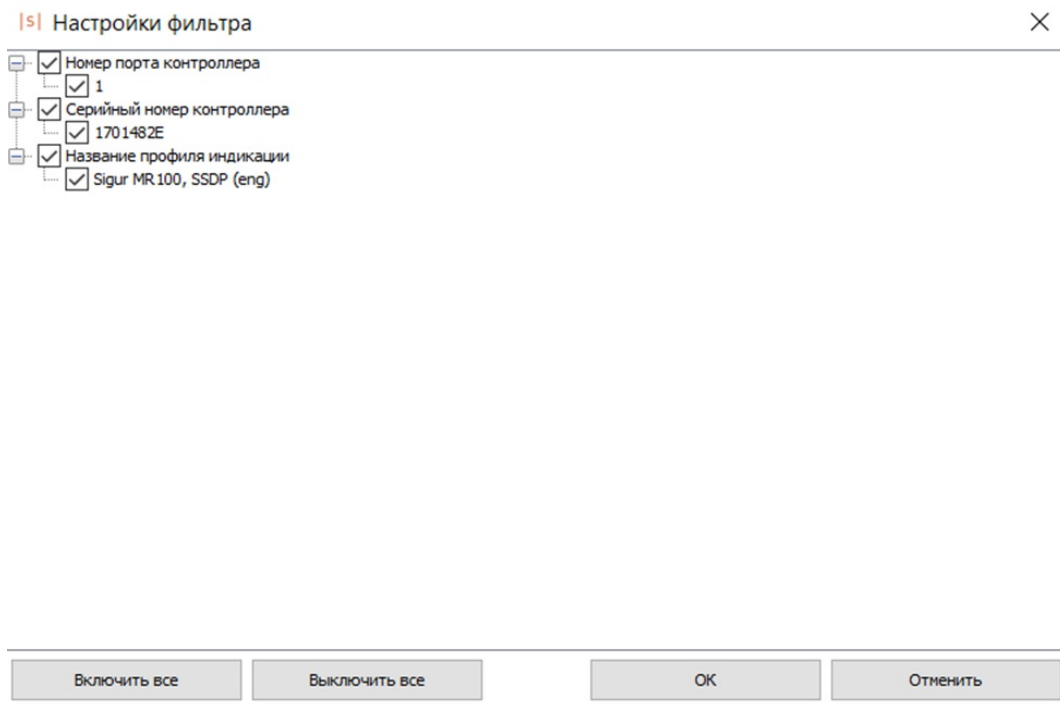
- «По параметрам». Данный фильтр можно настроить, нажав на кнопку



«Отфильтровать отображённые события».

С помощью фильтра можно отфильтровать отображённые события по таким параметрам как:

- номер порта контроллера;
- серийный номер контроллера;
- название профиля индикации.



Настройки фильтра по параметрам.

## 20. Общие требования к смартфонам и ПО

Для полноценной работы функций приложений «Sigur Доступ» и «Sigur Настройки» должны соблюдаться следующие требования:

- ОС Android 5.0 и выше (для обоих приложений) или iOS 9.0 и выше (только для приложения «Sigur Доступ»).
- Поддержка технологии BLE (Bluetooth Low Energy).
- Версия сервера СКУД Sigur 1.1.1.14.s и выше.



Производителем не гарантируется полная функциональность приложений на смартфонах с ОС Android. Например, некоторые смартфоны могут не поддерживать функцию идентификации при заблокированном экране. Это может происходить из-за физического отключения Bluetooth смартфона в силу особенностей данного устройства или его системной сборки.



В силу стандартных ограничений мобильных платформ идентификация в фоновом режиме или на заблокированном экране может переставать работать спустя некоторое время.



Приложения «[Sigur Доступ](#)» и «[Sigur Настройки](#)» используют сервис «Определение местоположения» смартфона. Включите данную функцию на вашем смартфоне и предоставьте соответствующие права на её использование приложениям.



При установке приложений на смартфоны под управлением ОС Android рекомендуется отключить для приложений контроль фоновой активности. Наличие такого контроля и возможность его отключения зависит от конкретного производителя, например: зайти в Настройки ОС - выбрать раздел Приложения - Все приложения - выбрать приложение Sigur в списке - найти опцию "Контроль активности" и установить её в значение "нет ограничений".

Сервис «Определение местоположения» используется приложениями Sigur для сканирования BLE-устройств вокруг. Такими устройствами являются считыватели Sigur.

Доступ к геолокации, в свою очередь, приложениями Sigur не используется: это описано в политике конфиденциальности к приложениям производителя [здесь](#) и [здесь](#). Таким образом, приложения Sigur не используют и не собирают информацию о физических координатах устройств.

Необходимость включения службы «Определение местоположения» для поиска BLE-устройств вокруг – часть архитектуры систем Android и iOS и является политикой компаний-разработчиков этих операционных систем.

- На устройствах с ОС Android версии 6.0 и выше сканирование BLE-устройств не работает без включенного модуля и предоставленных прав к функции «Определение местоположения».
- На устройствах с iOS не работает идентификация в фоновом режиме без включенной функции «Определение местоположения».

## 21. Логика обработки идентификаторов

### 21.1. Чтение карты

После поднесения карты поддерживаемого формата к включенному считывателю в область его чтения:

- Считыватель определяет формат поднесенной карты.
- В зависимости от заранее загруженной на считыватель конфигурации, определяет режим чтения карты по её типу: «Защищенный», «UID» или «Нет».
- Если настройка для данного типа карты не предусматривает её чтение, то считыватель не реагирует на карту: отсутствует какая-либо индикация считывателя, на выходной интерфейс не передаются никакие данные.
- Если настройка для данного типа карты предусматривает чтение UID, то считыватель пытается прочитать уникальный открытый код карты.
- Если настройка для данного типа карты предусматривает работу с защищенной областью памяти карты, то считыватель пытается авторизоваться в блоке памяти карты. Номер блока памяти и ключ указаны в конфигурации считывателя. В случае успешной авторизации считывается информация из данного блока памяти. В случае неуспешной авторизации никакой реакции от считывателя не последует: отсутствует какая-либо индикация считывателя, на выходной интерфейс не передаются никакие данные.
- После успешного чтения код карты передаётся на выходной интерфейс считывателя. В качестве кода передаётся:
  - для всех карт, кроме EM Marine и HID ProxCard II - N байт, определенных конфигурацией считывателя в прямом порядке: Wiegand-26 – 3 байта, Wiegand-34 – 4 байта, Wiegand-58 – 7 байт. В случае защищенного режима – это первые N байт блока памяти карты, без смещений. Если считанный код содержит меньше информации, чем определённая разрядность Wiegand'a, то код дополняется ведущими нулями. В случае идентификаторов Mifare Classic и Mifare Plus порядок следования байт зависит от настроек конфигурации, загруженной на считыватель.
  - для карт EM Marine и HID ProxCard II - 3 байта. Если конфигурацией определена передача фиксированного facility-кода, то правый байт заменяется на заданное в конфигурации значение.

## 21.2. Чтение смартфона

- Если приложение «Доступ» запущено, ему предоставлены соответствующие права, и на смартфоне включены функции «Bluetooth» и «Определение местоположения», то приложение пытается обнаружить считыватели Sigur MR100 или Sigur MR100 Multi.
- Если в результате сканирования было найдено несколько считывателей, то с каждым из них последовательно выполняются следующие операции:
  - Со считывателя приложение получает данные о его настройках:
    - Включен ли на считывателе режим чтения смартфонов;
    - Установленная дальность чтения смартфонов;
    - Политика срабатывания («Когда приложение на экране», «Приложение в фоне, экран разблокирован» или «Всегда»);
    - Режим чтения смартфонов: «не использовать», «базовый» или в «пользовательский»;
    - Уникальная информация о сервере, на котором создавался конфигурационный файл или мастер-карта для считывателя.
  - Идентификация будет произведена (смартфон «считается») в случае, если выполнены следующие условия:
    - Режим чтения смартфонов «Базовый» или «Пользовательский».
    - Состояние приложения и смартфона соответствуют политике срабатывания, установленной настройками считывателя (приложение в фоне, экран разблокирован и т.п.);
    - В случае BLE-идентификации:
      1. В приложении «Доступ» включен режим Bluetooth-идентификации.
      2. Показания мощности сигнала на антенне смартфона, наводимой сигналом с данного считывателя, больше по номинальной величине значения, установленного настройками считывателя (отрицательные значения dBm).
      3. Данный смартфон «не появлялся» в области чтения данного считывателя дольше 5 секунд. Под «появлением» стоит понимать не только физическое положение смартфона относительно считывателя, но и выполнение политики срабатывания в текущий момент на смартфоне. Например, если политика срабатывания на считывателе «Приложение на экране», то перевод приложения в фоновый режим работы аналогичен выходу из зоны чтения считывателя. Таким образом, если смартфон «появлялся», то каждое его «появление» увеличивает это ожидание ещё на 5 секунд. Если смартфон совсем не покидает область чтения, то идентификация произойдёт лишь один раз.
    - В случае NFC-идентификации:
      1. В приложении «Доступ» включен режим NFC-идентификации.
      2. NFC-модуль устройства был обнаружен считывателем.

- Сравнивается информация о сервере СКУД, с которого был запрограммирован считыватель с информацией о сервере СКУД, указанном в одном из загруженных «пригласительных» писем. Если считыватель работает в «базовом» режиме, этот шаг пропускается.
- После выполнения всех вышеуказанных условий, на считыватель передаётся идентификатор смартфона, который можно посмотреть в разделе «О программе» приложения «Доступ». Если какое-либо условие не выполняется, код не передаётся на считыватель.
- После получения считывателем идентификатора смартфона, его код передаётся на выходной интерфейс считывателя. В качестве кода передаётся N байт, определенных конфигурацией считывателя: Wiegand-26 – 3 байта, Wiegand-34 – 4 байта, Wiegand-58 – 7 байт.

## 22. Контакты

ООО «Промышленная автоматика – контроль доступа»  
Адрес: 603001, Нижний Новгород, ул. Керченская, д. 13, 4 этаж.

Система контроля и управления доступом «Sigur»

Сайт: [www.sigur.com](http://www.sigur.com)

По общим вопросам: [info@sigur.com](mailto:info@sigur.com)

Техническая поддержка: [support@sigur.com](mailto:support@sigur.com)

Телефон: +7 (800) 700 31 83, +7 (495) 665 30 48, +7 (831) 260 12 93